IAEA-TECDOC-1252

Information integration in control rooms and technical offices in nuclear power plants

Report prepared within the framework of the International Working Group on Nuclear Power Plant Control and Instrumentation

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

November 2001

The originating Section of this publication in the IAEA was:

Nuclear Power Engineering Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

INFORMATION INTEGRATION IN CONTROL ROOMS AND
TECHNICAL OFFICES IN NUCLEAR POWER PLANTS
IAEA, VIENNA, 2001
IAEA-TECDOC-1252
ISSN 1011–4289

Printed by the IAEA in Austria
November 2001

FOREWORD

The majority of the nuclear power plants in the world were designed 25 to 45 years ago. The information, instrumentation, safety, and control systems in these plant designs were based on analog, relay, and primitive digital technology. Computers that were available when most of the nuclear power plants were built were unsophisticated compared with those currently available. These less powerful machines with limited computational capabilities and memory were used to collect and store information. The main means for obtaining information from the plant were analog meters and strip chart recorders. In many cases these pieces of data had to be integrated and correlated with other data manually, in order to be usable. Procedures and plant information resided on paper only and were frequently hard to find and access in a timely manner.

This report provides guidance to help with the integration of information in order to enhance the usability and usefulness of the information. It can also be used to help avoid the pitfalls that can occur when implementing new systems with respect to the information they need and produce. This report's philosophy is based on three important issues that allow the convenient structuring of the problem and to keep all of its important features. The first issue is the process of information systems integration and use. This is achieved by long term planning and the creation of the plant infrastructure plan. The second is to take care of the end users' needs in relation to their abilities. This is realized through analyses of user needs. Third is the design of the human–system interface (HSI), for example to distinguish between types of information for use in the plant control room and in technical offices.

The development of this report was initiated by the IAEA International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI). It is a logical follow-up to IAEA-TECDOC-1016, Modernization of Instrumentation and Control in Nuclear Power Plants (1998). This report is intended typically for plant managers, project managers, I&C system designers, system engineers, operations managers, operators, and other plant information users.

This report is the result of a series of consultants meetings held in Vienna (April 1999, March 2000, October 2000). It was prepared with the participation and contributions of experts from the Czech Republic, Hungary, Norway, Sweden and the United States of America. In addition, a related Specialists Meeting on Integrated Information Presentation in Control Rooms and Technical Offices at Nuclear Power Plants was held in Stockholm, Sweden in May 2000. The experts, with the help of an expert from Germany, incorporated some of the lessons learned in the meeting papers into this report.

Special thanks are due to J. Naser (USA) who chaired the working meetings and co-ordinated the work. Ki-Sig Kang and A. Kossilov of the Division of Nuclear Power were the IAEA officers responsible for this publication.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. GENERAL INTRODUCTION

The majority of the nuclear power plants in the world were designed 25 to 45 years ago. The information, instrumentation, safety, and control systems in these plant designs were based on analog, relay, and primitive digital technology. Computers that were available when most of the nuclear power plants were built were unsophisticated compared with those currently available. These less powerful machines with limited computational capabilities and memory were used to collect and store information. The main means for obtaining information from the plant were analog meters and strip chart recorders. In many cases these pieces of data had to be integrated and correlated with other data manually, in order to be usable. Procedures and plant information resided on paper only and were frequently hard to find and access in a timely manner. Over the years, the demands for improved information access and presentation, and for improved calculation and storage capabilities have increased. The demands for access to information from sources outside the control room have increased substantially, while the need for improved integration and presentation of information has been the basic demand in the control room. This latter is accentuated by the reduction of the conventional, discrete instruments in the control room forcing the need for better information integration and ease of access to information that is no longer spatially dedicated. Fortunately, the processing, presentation, and storage capabilities of computers have also improved greatly.

The computerization of nuclear power plants has been implemented in incremental steps over time. In many cases in a manner that, while efficient for the specific system, is not the most beneficial for the plant as a whole. Several generations of computer technology may exist in the plant, which makes it difficult to transfer data between incompatible systems. Problems often arise when software applications need to be ported to new computer platforms. From the very beginning, the basic task to be achieved with computer technology was improved information access, integration, and presentation for the plant operations staff. The centralized plant process computer was the main capability to provide this information. However, since the capabilities of the older generations of computers were limited, they did not offer all of the desired information access, integration, and presentation. Therefore, these older systems were unable to offer the full potential of information to support the efficient operation of the plant. Over time, the computational capability has been constantly augmented through the implementation of different stand-alone systems such as the safety parameter display system (SPDS). Each of these new systems was developed and implemented to present the operations staff with new and better organized information about plant status, process trends, and equipment condition.

Over this same time, computers have also been introduced for information access and presentation to other categories of plant personnel including management, maintenance, and engineering staffs. Since the vast majority of these computer improvement projects were done stand-alone, they introduced a number of problems and inefficiencies and, in general, did not support a wide range of users. For example, it is difficult to guarantee the consistency of data presentation to different users when the same piece of information resides redundantly in several stand-alone systems. This potential inconsistency of information can have detrimental effects on plant operation and can even create a situation that challenges the safety of the plant. The overall need for modernization of the information, instrumentation, safety, and control systems in nuclear power plants offers the opportunity to develop and implement new computer systems, networks, and displays that will effectively access and present the full range of information required by all categories of the plant staff. This will assist them in operating the plant more efficiently and safely. The typical users of information in an integrated environment can be seen in Fig. 1. In order to highlight the benefits of information integration, examples of applications using the methods described in this report are included in Section 9.

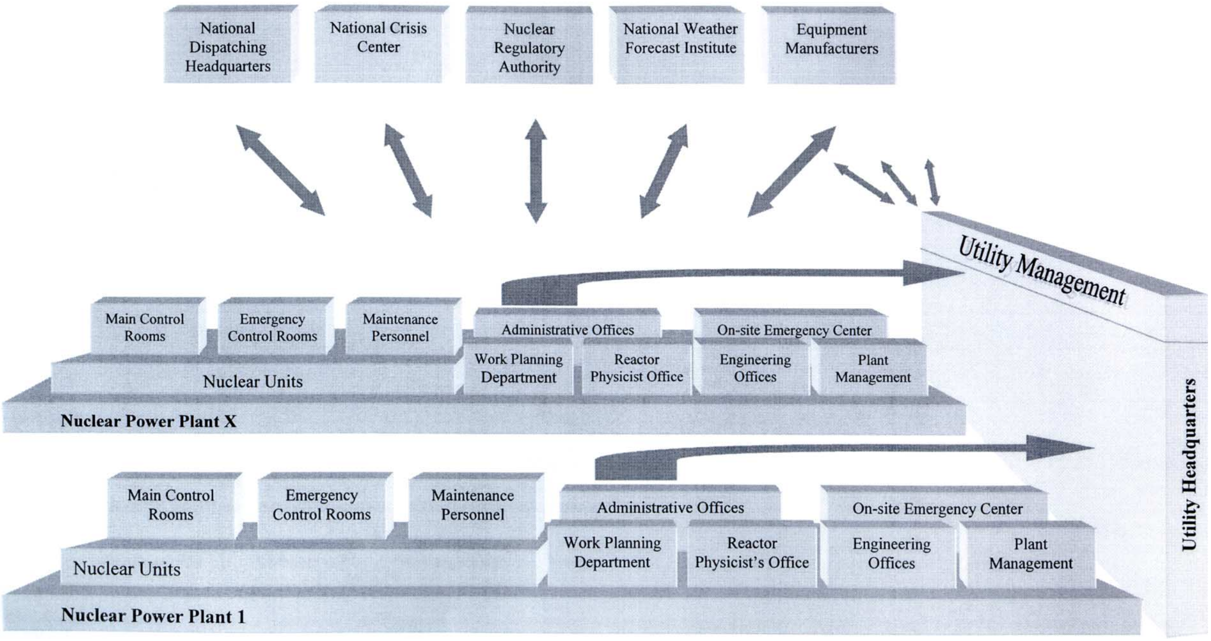

FIG. 1. Typical users of information in an integrated environment.

1.2. PURPOSE AND SCOPE

This report is intended typically for plant managers, project managers, I&C system designers, system engineers, operations managers, operators, and other plant information users. The topics addressed in the report are mainly applicable in operating plants both for entirely new, or modernized I&C systems.

The report will provide guidance to help with the integration of information in order to enhance the usability and usefulness of the information. This report can also be used to help avoid the pitfalls that can occur when implementing new systems with respect to the information they need and produce. Although most of the above applications are for the plant, it is important to consider the off-site needs for information. Such off-site users of information are; for example, the corporate and engineering offices of large utilities running many plants, and national regulatory bodies that request continuous transfer of key plant parameters important to safety.

Another purpose of this report is to collect the best practices in certain areas of special interest and to offer guidance in the complex environment of distributed digital and software oriented systems implementation. Where appropriate, the report gives references to standards, guidelines and other documents, where more details can be found.

This report's philosophy is based on three important issues that allow the convenient structuring of the problem and to keep all of its important features. The first issue is the process of information systems integration and use. This is achieved by long term planning and the creation of the plant infrastructure plan. Second, is to take care of the end users' needs in relationship to their abilities. This is realized through the analyses of the user needs. Third is the design of the HSI, for example to distinguish between types of information for use in the plant control room and in technical offices.

1.3. RELATION TO RELEVANT ACTIVITIES

Nuclear power plants, along with other power producers in the electric power industry, are under great pressures to operate cost-effectively. In countries where deregulation is already or will become a reality, it is important to improve the plant's competitive position to be a power supplier of choice. In countries where deregulation is not a reality, minimizing the cost of the power production is also an important objective. Another major concern for nuclear power plants is maintaining or enhancing the highly safe operation of the plant. For many operating plants modernization of instrumentation and control (I&C) systems, plant process computers, and control rooms is becoming a necessity for improving the cost-effective operation and for replacing obsolete equipment. A report on modernization of I&C systems developed by the IAEA [1] has done a thorough job in describing the issues and recommended processes for modernization activities. Many of these same processes apply to new plants as well. Guidance on human–system interfaces can be found in Ref. [2].

Important contributors to cost-effective and safe operation of nuclear power plants are data and integrated information. Accurate and effective access, integration, correlation, presentation, and use of data and information is a major contributor to reduce operations and maintenance (O&M) costs, to improve plant performance, to enhance safety, to reduce the potential for human errors, and to improve competitiveness. Modern technology provides the tools to obtain, integrate, and present information at levels that were not possible when many of the current plants were built. Easy and timely access to accurate, integrated information strengthens decision-making, improves productivity, improves quality, and reduces overall costs. In addition, there is the prevailing direction in some countries to reduce the personnel at plants forcing fewer people to perform the same or more activities than previously done by larger staffs. Information, and the effective use of it, is the only way to achieve this without degrading the competitiveness or safety of the plant. A well-designed integrated information system is needed to provide processed data at the right level of information to be used by plant personnel in the most efficient way for carrying out their tasks. Therefore, effective access and integration of distributed information is essential for the efficient and safe operation of the plant. In competitive environments, it is essential for the economic survival of the plant.

1.4. STRUCTURE OF THE REPORT

Section 2 gives the background situation of information development and presentation in nuclear power plants. Section 3 provides the key elements in a systematic and integrated approach. It also describes long term planning of the plant information infrastructure. Section 4 describes the key elements for creating architecture and an environment that will make information available to the user in a manner that is transparent to him or her regardless of where the information and functions physically reside. Section 5 depicts how analysis methods can be used in order to achieve user driven solutions. Section 6 outlines how information integration can be mapped to a system life-cycle. Section 7 points out important aspects of the human–system interface, important considerations about alarm system applications, as well as the security and integrity of information. Section 8 describes tools and methods that can be used to support the specification, design, and verification and validation of a system. Section 9 contains examples of situations where information integration can be beneficial utilizing the methods discussed in this report. Section 10 lists lessons learned from real projects. Section 11 gives recommendations.

2. BACKGROUND

The majority of the nuclear power plants in the world still have the greater part of their original analog and aged digital instrumentation and control (I&C) equipment in operation. Many of the I&C systems in the plant need to be modernized in a reliable and cost-effective manner to replace obsolete equipment, to reduce operations and maintenance (O&M) costs, to improve plant performance, to enhance safety, and to improve competitiveness.

Major drivers for the modernization of I&C equipment are the need for more cost-effective power production, for improved competitiveness, and for replacing obsolete equipment. In addition, plants, which are pursuing life/license extension, need to modernize equipment to enable a number of the systems to satisfy the extended operation requirements, and in some cases the more stringent licensing requirements. Competition between power producers, especially in countries where deregulation is occurring, is dictating the need for more cost-effective and reliable power production. Deregulation and other competitive forces are challenging nuclear power plants to become more efficient and competitive, while at the same time maintaining or improving plant safety. It is also a pressure from the environment that the nuclear industry should be pro-active in maintenance and modernization of their plants. To obtain public acceptance, the society expects nuclear power plants to take optimal benefit of technology advances (including information technology) as seen in competing industries producing power by conventional means and as performed by the industry in general.

Accurate, easily accessible, and well-presented information is the keystone to the efficient and safe operation of the plant. Effective use of modern technology is the facilitator for obtaining this information. Based on the more intense competition between energy production sources, usually fewer resources are available to operate the plant. In many cases plant staff are being reduced for economic reasons. At the same time, it is necessary to run the plant more productively. Therefore, more is required to be done with fewer financial and personnel resources. Wide use of high quality information will support doing a better job with fewer resources. Therefore, information is essential, and is becoming even more so, for the efficient and safe operation of the plant. In competitive environments, it is essential for the economic survival of the plant.

Modern computer technology offers the ability to easily store, easily access, and effectively present information of high quality to all categories of plant staff to assist them to do their jobs more effectively. Replacement of obsolete plant computers and the need to modernize the information, instrument, control, and safety systems provides a golden opportunity to design and implement enhanced computer and network technology to support plant staff. This modern technology will allow the user to obtain any information and applications he needs to do his job from his own workstation in a manner that is transparent to the physical location of the information and application. This modern technology will allow the presentation of the information in a manner that is more supportive to the user and is less prone to introduce errors if properly designed and implemented.

Easy and timely access to accurate information strengthens decision making, improves productivity, improves quality, and reduces overall costs. Modern computer and network technology facilitates the need to have the right information to the right person at the right time to allow the correct and efficient performance of the person's job. The goal is to provide a good integrated information technology work environment and avoid that personnel spend their time on trivial tasks like data gathering and data conversion. Some utilities have reported that as much as 50% of the operating staff's working time is required to search for information and to compile that information in a form that is useful and usable. In general, this is not what operating staff should be spending their time doing. Instead they should have ready access to the correct information to allow them to monitor the plant's operation and make the appropriate decisions for effective and safe operation.

New technologies offer significant opportunities to improve the access and presentation of information to the user. However, this technology should be used judiciously. Modifications to the plant should be made for the benefit of the plant to introduce solutions to the needs of the plant and its staff. New technology should not be introduced just to have the latest and greatest capabilities. This technology driven approach often appears impressive and attractive, but is frequently not effective and can be very costly. The user-driven approach is more effective and more stable than trying to chase technology, which is changing so rapidly. To obtain viable solutions, the user should be involved in the whole life-cycle and, in particular, the user should be consulted at an early stage when the project planning, organization and staffing are established. This is to ensure that all end-user needs and requirements are uncovered and considered throughout the project life-cycle.

The purpose of a well designed integrated information system is to provide processed data at the right level of information to be used by plant personnel in the most efficient way for carrying out their tasks. Due consideration should be given to the design of the computer architecture and network to ensure efficient transfer, conversion and sharing of data among plant personnel. Internal networks and Internet usage are now widespread and well accepted technologies as means for information sharing, and the challenge for the nuclear industry is to apply this technology in the right way. Sufficient flexible and expandable solutions should be offered to allow adaptations to end-user's needs as they may appear in the future, without having to reconstruct the whole information system. The integrated information approach should be designed and prepared for changes both from users and technology.

3. GENERAL APPROACH

3.1. KEY ELEMENTS FOR A SYSTEMATIC APPROACH

As needs in the plant have arisen for improved computational capabilities and information access and presentation, plants have usually made these improvements to satisfy the particular needs of the specific project at hand without taking into consideration the needs and goals of the plant as a whole. This means that new systems have been implemented and maintained in a stand-alone manner supporting a particular application and group of plant staff. This has led to isolated islands of functionality and information, which hinder access and free exchange. It has created an environment of unnecessarily redundant information and functions, which can lead to problems of inconsistency as well as additional costs to develop and maintain. This environment also creates a situation where it is difficult to integrate information and functions, adapt to new needs, and to add new integrated systems and information. A systematic and integrated approach that takes into account the needs and constraints of the entire plant is needed. This approach is instrumental in addressing two major concerns in the plant that can challenge the safety of the plant as well as reduce the productivity. The first is the incorrect interpretation of information. The second is the inconsistency of the conclusions from information by different people or groups of people in the plant due to either inconsistencies in the information itself or inconsistencies in the interpretation. Both of these concerns can be addressed by the proper processing and presentation of integrated information to all groups.

The key elements in the systematic approach are:

- The creation of a long term infrastructure plan to ensure that integration is achievable and to facilitate the inclusion of new systems;
- Mapping information integration activities into the life-cycle of a project to ensure that the new system or function will be in compliance with the infrastructure plan;
- Use analysis techniques in order to make sure that the solution will be user driven.

3.2. LONG TERM PLANNING

A long term plant infrastructure plan should be developed based on the needs and constraints of the plant as a whole. This plan should also consider other ongoing and planned activities in the plant and coordinate with those activities as appropriate. This plan will identify the current infrastructure, the desired infrastructure at the end of the plan’s period of interest, and develop a migration schedule to form the phases of the steps to achieve the long term goals. Then new functionality, displays, and information sources will be added in a manner consistent with this long term infrastructure plan to ensure that integration is achievable and to facilitate the inclusion of new systems and information. An additional benefit of this integrated approach and infrastructure is the ability to have a single information source for each piece of information when there are not other reasons such as safety/non-safety information isolation requirements, which require multiple sources. This does not imply that there will be only a single value for a parameter if there are multiple sensors measuring that value, but that the measured value of each sensor will be stored in as few places as possible. Doing so removes both the potential inconsistencies of unnecessarily storing the same data in multiple locations, and the need for extra memory locations and links. Since the information is now available to all functions and users, there is no longer a need to have it reside unnecessarily in several locations. This eliminates the concern of data inconsistencies and the potential productivity and safety problems to which that could lead. This integrated infrastructure also facilitates the combination of information into a form that is more meaningful to the user. The plant infrastructure plan should give guidance for consistent human–system interfaces as well as guidance on how to achieve adequate data security.

The preparation of the long term plant infrastructure plan is discussed in detail in Section 4.

4. PLANT INFRASTRUCTURE PLAN AND PLANT INTEGRATION ENVIRONMENT

4.1. INTRODUCTION

The current situation in most plants is best described as being a distributed computer system solution as opposed to a centralized computer system solution. This refers to the fact that plant information resides in many distributed locations, the functionality to take that information and compute results needed by the plant staff is distributed, and the staff requiring the information and computed results are also distributed physically. Information integration is needed to enhance the capabilities of systems and to allow the user to perform his job more effectively. However, the ability to integrate information in a cost-effective and user-friendly manner does not just happen. It requires a communications and computing architecture to physically allow it to happen. It also requires an integration environment to allow the integration of the information and functionality from distributed sources to be available to the user.

This architecture and environment should be created to take the distributed information and functionality and make them readily available to the user in a manner that is transparent to the user as to where the information and functions physically reside. The user should be able to sit at his workstation and do whatever he needs to do to accomplish his job as if all of the information and functionality resided on his workstation. This combination of architecture and environment consists of networks, computers, display devices, and tools to allow the user to sit at his workstation and effectively perform any job that he needs to do. The development of this architecture and environment is necessary to cost-effectively do information integration and functionality combination from distributed sources.

Prior to the implementation of new I&C systems or the modernization of existing systems, a plant infrastructure plan should be developed to define the necessary communications and computing architecture for the plant. The existing system infrastructure will have a significant effect on this plan, especially if the changes in the architecture will be done in an incremental manner. Similarly, when working in a distributed environment, a plant integration environment should be defined to allow the transparent access to distributed information and functionality that is required by the user to do his job. This environment is needed to support the user-friendly integration of both information and functionality. One necessary concern of this plant integration environment is information and functionality access control. While the environment supports transparent access when it is needed, it is also designed to prevent unauthorized access.

4.2. PLANT INFRASTRUCTURE PLAN

Most nuclear power plants have become computerized through evolution rather than overall system planning. Each I&C or computer system was considered separately, without analyzing the interactions of adjacent and interrelated systems. Problems resulting from the evolution of non-integrated I&C systems are having a detrimental effect on the performance, connectivity, and maintainability of these systems and their information. Therefore, many nuclear power plants are suffering from one or more of the following problems:

(1) Isolated islands of computing due to the reality that plant systems and computers currently do not have communications with other systems and computers. In order to facilitate integrated information where needed, these systems need to participate in a plant-wide network. However, the systems should be put onto the plant network in a planned manner to avoid compatibility and interface problems.

(2) Inefficient and incompatible network protocols exist since currently large numbers of heterogeneous systems are networked together in a manner that was most convenient for each individual system without considering the overall plant solution. Typically, plant architectures have evolved by linking a pair of computers or systems together and then another pair and so on. This resulted in many small networks, often using several transmission media and network protocols. This requires that the implementers of modernized systems need to retrofit a number of the systems with a common transmission medium and protocol or that numerous routers and gateways be installed to convert the existing protocols.

(3) Saturated networks caused by the networks being put together without an overall plan. In many cases the problem is not that the network is too small but rather the amount of information placed on it is greater than actually needed. This occurs for two reasons. First, the network architecture structure may be without hierarchy so that each system places all of its communications traffic on the network. There is no hierarchy to filter information between levels. Second, the network was implemented poorly without regard to the isolation of local traffic. In addition, an inappropriate network technology may have been implemented. The designers may have relied mostly on the manufacturer's specifications and recommendations based on theoretical maximums of bandwidth. In reality; however, these theoretical bandwidths are rarely achieved.

(4) Unnecessary duplication of information and functionality is common where networks have evolved rather than been planned. This occurs before networks are implemented, since each system had to generate its own functions and information. Even in a networked system, the same duplication can occur when there are no guidelines or an overall plan to help designers recognize that information and functionality already exists and is accessible. It is important to note that there are reasons why a function or piece of information should be duplicated. For example, a piece of information needed for a safety system and for a control system may need to reside in two separate locations to assure safety/non-safety isolation or to assure that the time response of the safety and control systems are both within specifications. This problem refers only to unnecessary duplication and is not to be interpreted as a requirement that there is to be a single source for all functions and information.

(5) Inconsistent human–system interfaces amongst systems can lead to training problems, overly complex or confusing user tasks, user fatigue, or user errors. The inconsistent HSI is caused by a lack of guidelines that define acceptable HSIs for specific types of systems and information. This does not necessarily mean that there should be a single HSI for all systems, because the user knowledge and tasks in the specific project must be considered.

(6) Difficulty or inability to migrate to new computer platforms and I&C systems in the future. Without guidelines to support flexibility and expandability, it is difficult to implement new and modernized systems and their information into the existing environment.

In order to avoid the types of problems identified above, a long term plant information plan should be developed taking into account the overall needs and goals of the plant. This plan defines how I&C systems and the plant communications and computing architecture should be implemented in a cost-effective and controlled manner during a plant specified period of time. The plan will define the characteristics of the computers and information to be used in future systems, how they and other process control equipment will be connected, and the look and feel for HSI.

An example of an approach for developing this long term plan is the Plant Communications and Computing Architecture Plan Methodology [3, 4]. The objective of this methodology is to develop a long term plan for implementing an architecture, in which:

- Each I&C system will be able to communicate effectively with other internal and external systems.
- Isolation of safety systems and information so that they cannot be corrupted by other systems or information.
- Access control for data security.
- The HSI of each modernized I&C system will be consistent in the look and feel with the other modernized systems.
- Future migration to new hardware or technologies can be achieved without excessive downtime or a major conversion effort.
- Each modernized I&C system will be able to take advantage of additional functionality available with newer technologies and will also integrate smoothly with older systems in the plant.
- The migration to the new architecture is scheduled in phases that are coordinated with other plant events such as plant outages.
- Information and functionality will not be unnecessarily duplicated.
- Integration of information will be facilitated.
- Inefficient or incompatible existing network protocols will be phased out as much as possible.

This methodology has several steps that will lead to the overall plant information plan.

The first step is to determine the overall objectives, assumptions, constraints, and goals for system and information integration.

The second step is to identify all existing projects and plans to see how they will affect the new architecture. These existing projects and plans also identify opportunities. For example, a plant process computer replacement is an excellent opportunity for putting in new networks and philosophies for information sharing and integration.

The third step is to look at the existing and planned future I&C systems and information. For the existing systems, each system is identified either as a system that is a candidate for modernization, a system that will not be modernized but will communicate with an expected modernized system, or a system that is not expected to be modernized or to communicate with a system that is expected to be modernized. The plan will have to include support for all of these systems. For future systems, each new system or system expected to be modernized is identified along with their information needs and production as well as opportunities for information integration. Finally, a first estimate of the modernization schedule over the planned period is developed.

The fourth step is to develop the approved strategy for the implementation of new and modernized systems. This includes guidance on the characteristics of the computing platforms and process control equipment. This will provide the framework for I&C modernization engineers to develop consistent solutions across similar systems.

The fifth step is to describe the current network configuration and to develop the future network configuration, including protocols, physical topology, data flow, and data security. The future communications architecture will include a network communications model and a phased implementation schedule.

The sixth step is to develop an HSI plan (see Section 7.2.2) as part of the plant infrastructure plan. This gives the basic common HSI requirements, including the desired look and feel for all future systems. As the plant infrastructure plan is a living document, user experience should be fed back in order to update the HSI portion of it to continue to satisfy users' needs. The HSI for a project needs to follow the rules set up in the HSI plan in order to assure consistency.

The last step is the development of the guidelines for the characteristics of the computer platforms to be used for future systems. Similarly, guidelines need to be developed for the process control equipment.

The preparation process of the plant infrastructure plan is depicted in Fig. 2.

The plant infrastructure plan will identify a plant specific solution that will support the integration of systems and information in the plant. This will facilitate the connection of systems and the sharing and integration of information in an easy to implement and flexible manner. It also supports easy expansion when new systems, information sources, and workstations are added. By identifying open protocols and common data structures, it will be easy to implement new integrated systems and information without developing special interfaces between them. In addition, this solution will reduce the number of special interfaces between existing systems to allow integration and it will also simplify these special interfaces. The number of interfaces will be reduced since each system to be integrated with others will not have to be linked to each one individually. Instead each system and information source will interface to the common networks only. Since all of the systems and information sources that need to be connected will be similarly connected, they will have access to each other. In addition, the interfaces will be simpler since they will all interface to the same networks rather than to all possible combinations. This will be clarified in Fig. 3 (a, b, c).

Text cont. on page 14.

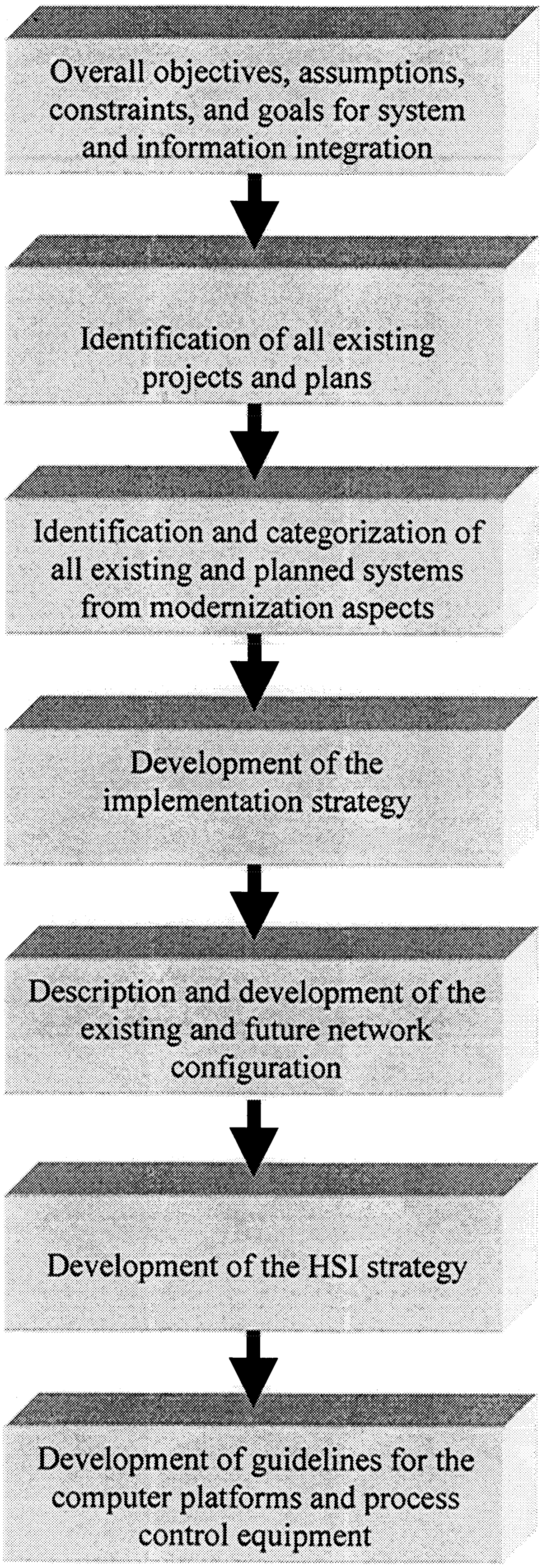
Overall objectives, assumptions, constraints, and goals for system and information integration
Identification of all existing projects and plans
Identification and categorization of all existing and planned systems from modernization aspects
Development of the implementation strategy
Description and development of the existing and future network configuration
Development of the HSI strategy
Development of guidelines for the computer platforms and process control equipment

FIG. 2. Preparation process of the plant infrastructure plan.

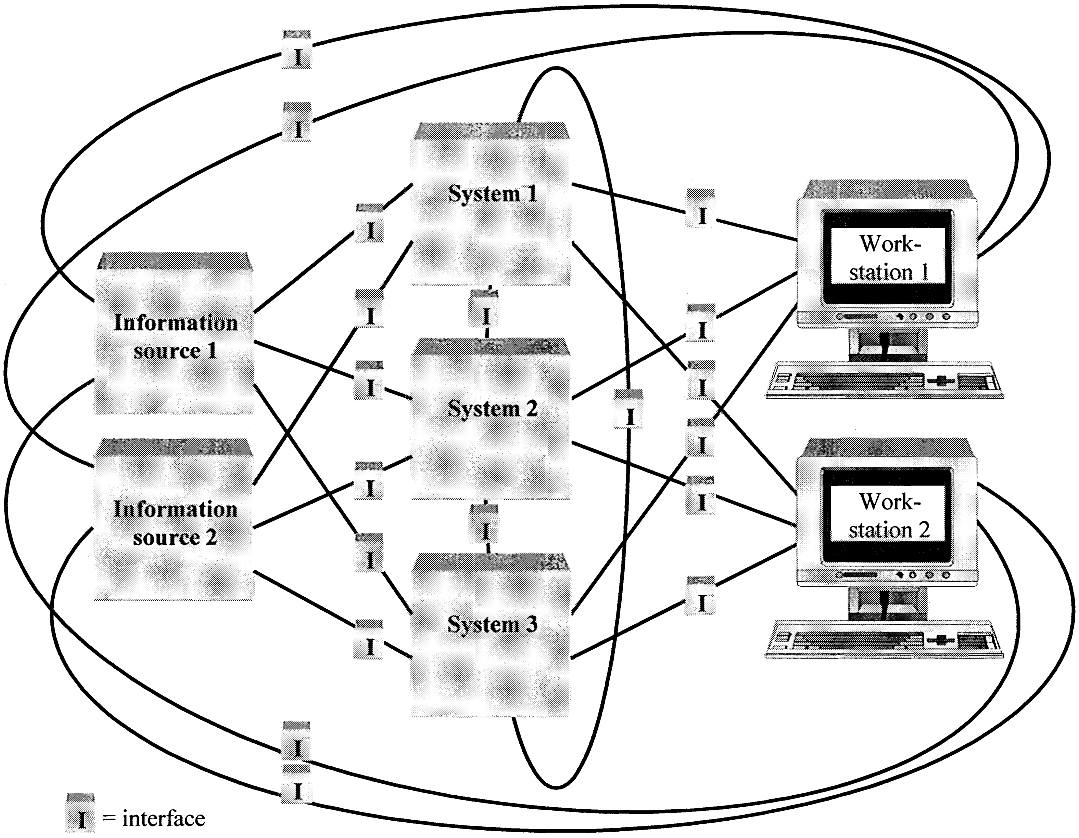

FIG. 3 (a). Network connections where no infrastructure plan exists.

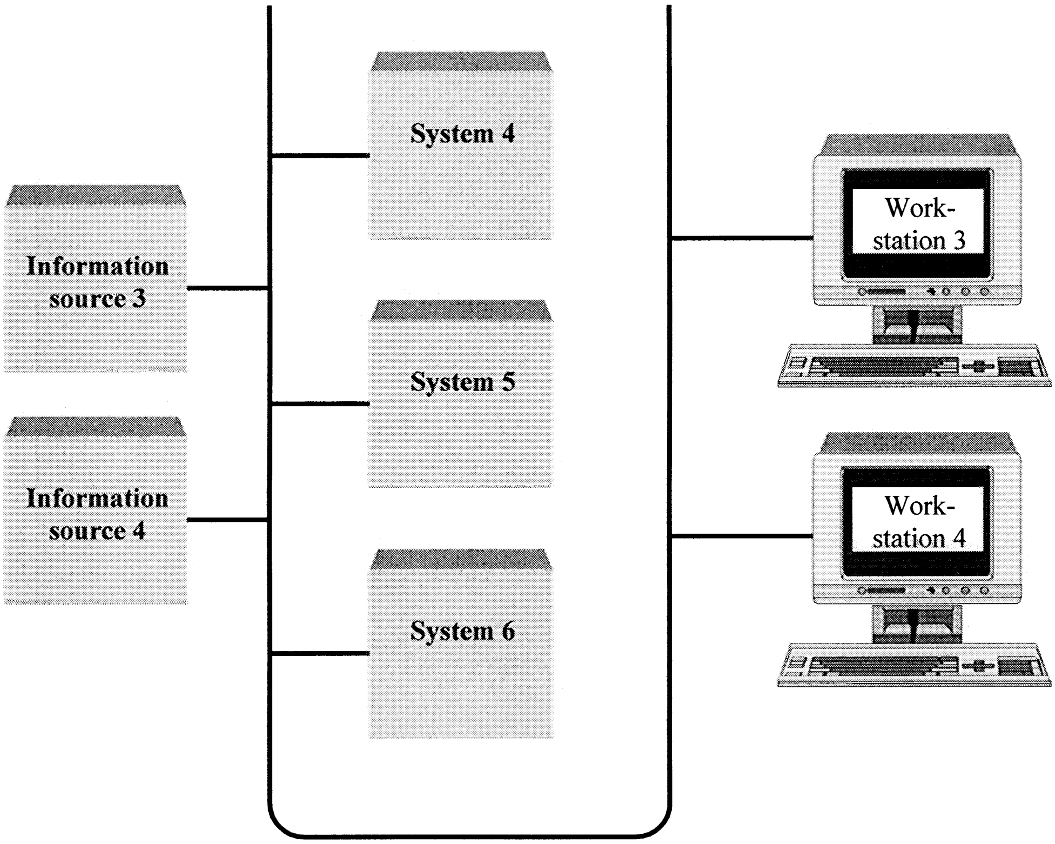

FIG. 3 (b). Network connections using infrastructure plan (simplified).

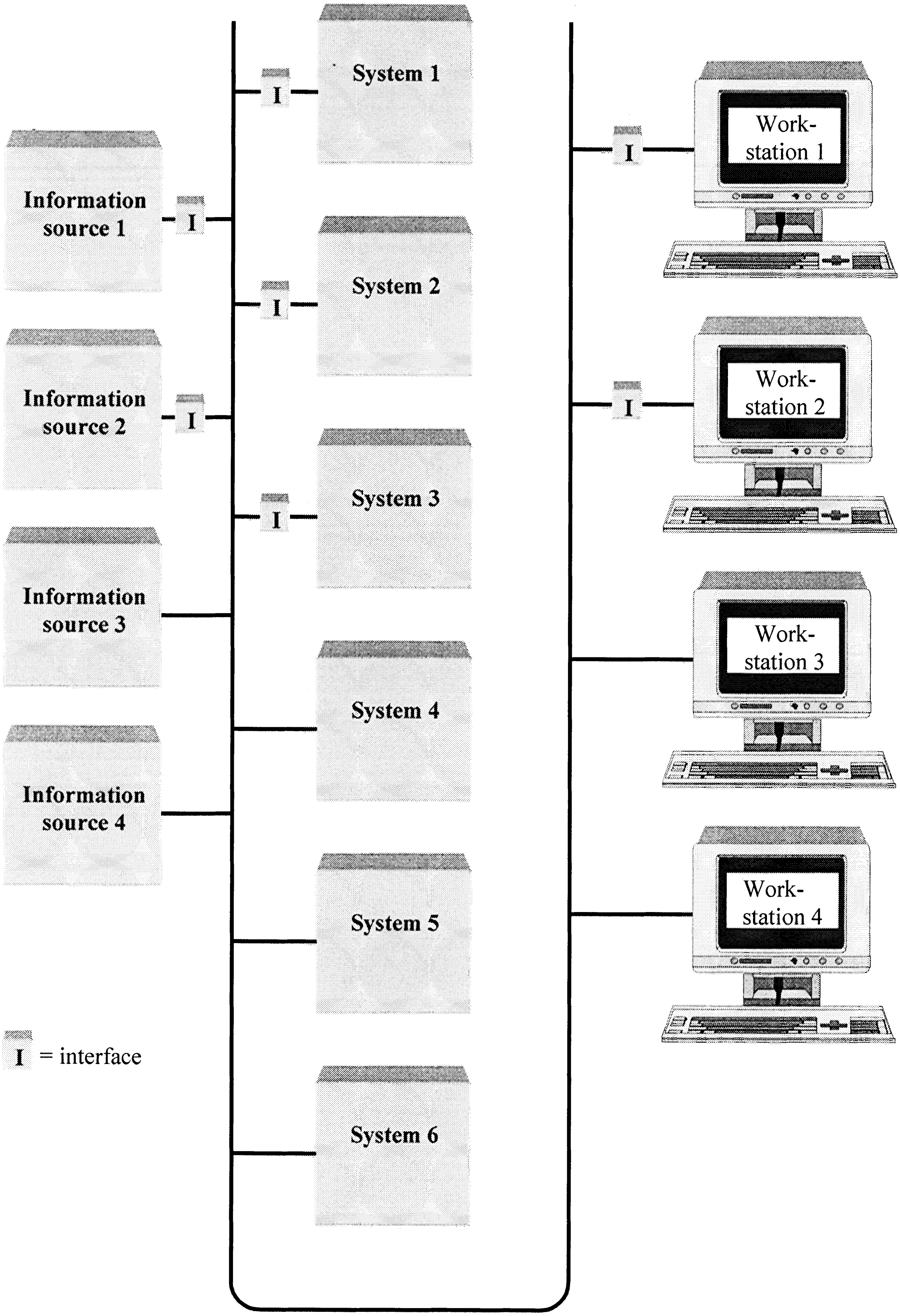

FIG. 3 (c). Network connections using infrastructure plan: accommodating components installed both before and after the plan was implemented (simplified).

Figure 3 (a) illustrates the situation where there is no common solution to support the integration of systems and integration. This figure illustrates the case where there are two distributed information sources, three distributed systems, and two workstations. In this case, it is desired to have all possible linkages between each of the components (systems, information sources, and workstations) with the exception that the two information sources are not linked together and the two workstations are not linked together. To do these desired interconnections without a planned architecture will require 19 direct links, and each of these in the worst case will require a specially written interface. This solution is both complicated and costly. If additional components are added, the complexity and cost grows rapidly. For example, adding one new system, which needs to be connected to all of the other components and assuming none of the protocols match, requires 7 new direct links and 7 new interfaces.

With a planned infrastructure of networks and agreed upon protocols, the situation is much simpler as shown in Fig. 3 (b). Here there is a network in place and protocols for each component and the network are consistent so that special interfaces are not required. In this case all that is needed is a network, and the components are connected as nodes on the network. As new components are added, they also become nodes on the network. For a real plant, this figure is an oversimplification but is used to clarify the concept. In the real plant more than one network will be required; for example, to isolate safety systems from non-safety I&C systems and both of them from information systems. One way links will be required to take information from the safety network to the control and information networks without allowing any potential corruption of the safety systems and information from the non-safety systems and information. A more realistic, though still simplified, example of an actual plant infrastructure is shown in Fig. 4.

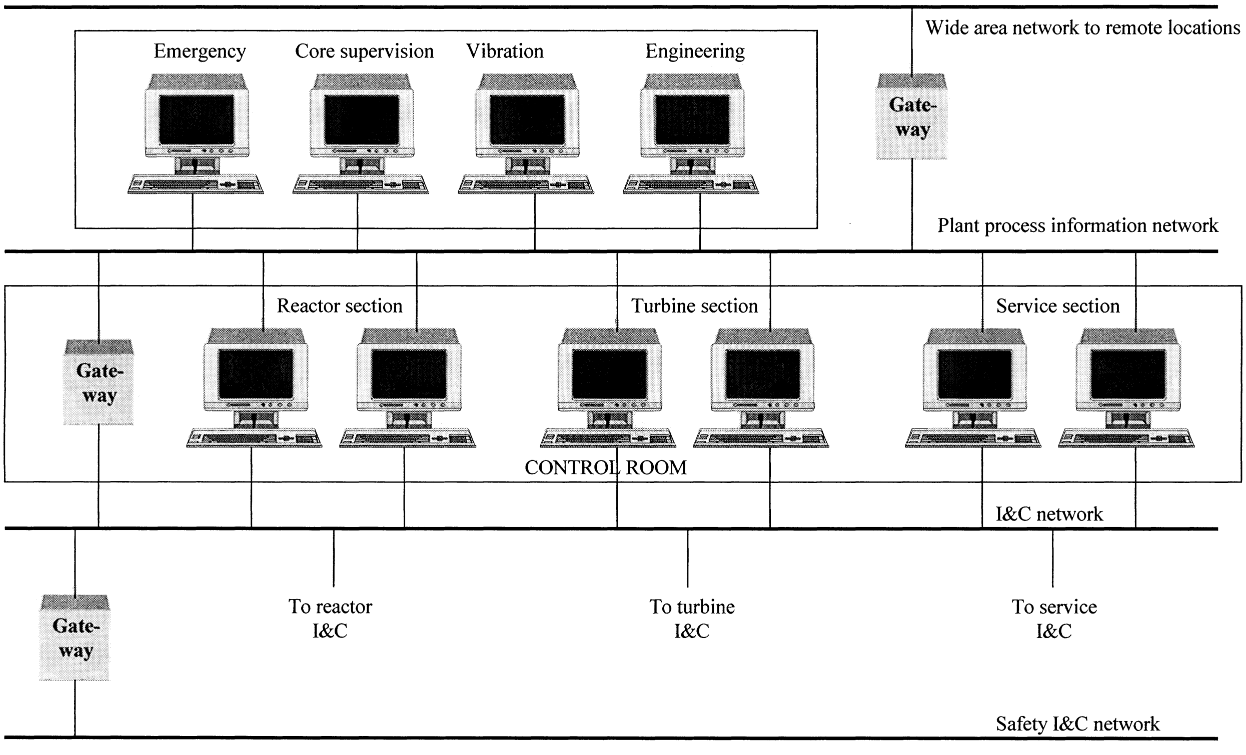

FIG. 4. Simplified example of an actual plant infrastructure.

From a practical point-of-view, the plant will be made up of systems, information sources, and workstations implemented before the plant infrastructure plan was developed. Other systems, information sources, and workstations were installed after the plan was developed and are consistent with the plan. The plant infrastructure plan should accommodate both of these sets of components. Assuming that one network is sufficient for illustration purposes, Fig. 3 (c) shows the architecture that accommodates both sets of components. Again the components that are consistent with the plan are just nodes on the network. The older components, which are not consistent with the plan, are attached directly to the network through a specially written interface for that component. There are only as many interfaces required as there are components in the worst case and these have more commonality than the interfaces above, as well as being fewer, since the target of each is the same network.

It is important to recognize that the plant infrastructure plan should be a living plan. This means that the plan should be reviewed periodically to ensure that it still addresses the plant's current goals, objectives, systems status, available equipment, etc. Based on the changes at the plant, on the changes in the utility's perspectives, on changes in technology, and on changes in the availability of equipment, it will most likely be necessary to modify the plan to address the new realities. This periodic review and plan modification is important to make sure that the new systems and architecture continue to effectively address the needs of the plant and plant owner.

4.3. COMMUNICATION MODEL

An important aspect of the infrastructure is the communication model. The communication model will identify and describe the information and protocols used to pass that information between users, systems, and functions. It will be used to analyze and verify that all of the required information is transferred within the time constraints for all operational situations.

To support a more cost-effective approach for linking components together, a communication model and a set of protocols in the model should be selected for the plant. It is recommended that an open system model be selected so that the likelihood of getting components to easily interface within the architecture is greatly enhanced.

The most commonly used open communication model is the Open Systems Interconnection (OSI) Reference Model [5]. This model is organized as a series of seven layers, each addressing specific communications functions. The layers are built upon each other, such that any given layer offers certain services to the higher layers, shielding those layers above from the details of how the offered services are actually implemented, and uses services of the next lower layer. In general, layers 1 through 3 (physical, data link, and network, respectively) define machine-to-machine communication; layer 4 (transport) defines end system to end system communications; and layers 5 through 7 (session, presentation, and application) define user oriented functionality. These layers are described in the following:

- The physical layer provides the data path between communicating data link entities. It is responsible for the transparent transmission of an arbitrary bit stream between adjacent data link nodes over some form of physical media.
- The data link layer is responsible for the error-free transmission of data between two adjacent OSI systems. It accomplishes this by performing functions such as error-checking and recovery, sequence checking, and flow control.

- The network layer provides the routing and relaying of data between the communicating systems. To accomplish this, this layer uses knowledge of the network topology to deliver the data to the proper end system.
- The transport layer is responsible for the end-to-end delivery of data packets between communicating session entities. It uses the routing services of the network layer and adds functions for efficiently moving the data, insuring its correctness and order, and insulating the session layer from data delivery concerns.
- The session layer organizes and manages dialog sessions between end users such that data and control information are transferred in an organized and synchronized manner. This is done by providing mechanisms to establish, maintain, and terminate sessions.
- The presentation layer is to provide for the common representation of data between end systems. This is achieved via the use of abstract syntaxes, which describe the data types and acceptable values to be transferred and of transfer syntaxes, encoding rules that define the bit level representation required to encode the data.
- The application layer is responsible for providing the window, or access, to the services provided by an open systems communications architecture. It provides both common elements for the management and activation of communication resources and specific elements for maintaining the context of the communication. The combination of these services allow, for example, the underlying OSI based communications resources to support the transfer of files between two end systems and interactive work station access from a work station to a remote host.

The protocols to be used in these seven layers need also be identified. An example of a set of protocols that have been selected to satisfy the specific needs of a nuclear power plant (as well as protocols for corporate, control centers, other power plants, transmission, distribution automation, and customer interfaces) is given in the Utility Communications Architecture [6].

New industry standards are emerging in the area of distributed computer systems, which will have large influence for future integration of applications in technical offices at nuclear power plants. It extends an object oriented programming system by allowing objects to be distributed across a heterogeneous network, so that each of these distributed object components operate together as a unified whole. These objects may be distributed on different computers throughout a network, living within their own address space outside of an application, and yet appear as though they were local to an application.

Three of the most popular distributed object paradigms are Microsoft's Distributed Component Object Model (DCOM), OMG's Common Object Request Broker Architecture (CORBA) and JavaSoft's Java/Remote Method Invocation (Java/RMI). These three paradigms fulfill the requirements of the OSI application (fourth to seventh) layers. They represent a major improvement in achieving information integration on the application layers.

4.4. DATA MODEL

A nuclear power plant has a large number of instruments that deliver a continuous stream of data throughout the whole plant life. Several application programs are consumers of this raw data and calculate more data and higher level information for decision-makers throughout the plant. As application programs are expanded, new calculation modules are introduced and data is shared, it is important to describe carefully the different data items on-site.

A data model will:

- Ensure consistent naming conventions and the uniqueness of data items.
- Reduce the chance of providing wrong data to an application program.
- Provide a means for avoiding multiple definition and unnecessarily redundant storage of data.
- Facilitate the integration of data.
- Simplify the interfacing of application programs.
- Reduce the danger for misinterpretation of the data by end users.
- Facilitate maintenance of application programs.

An example of the single, uniform interface requirements to access data stored in a variety of data systems found in the plant and the overall utility environment is given in the Database Access Integration Services [7]. This single, uniform interface is a common data model that includes a data representation formalism and data manipulation services. The data representation formalism is used to describe the structure of data. It includes basic data types such as character strings, integers, floating point numbers, dates, and times. It also includes aggregated data types such as structures, databases, and bit streams. The data manipulation services are used by applications to access remote databases. It includes both read and update capabilities. It accesses data according to its content or its location in a data system and allows merging and correlating data.

4.5. PLANT INTEGRATION ENVIRONMENT

After the plant communications and computing architecture has been defined by the plant infrastructure plan, a plant integration environment is needed to facilitate access to distributed pieces of information, access to distributed functions, and the tools to integrate both information and functionality. This will provide the user with what he needs to do his job. An illustration of this is given in Fig. 5. Here various types of information such as plant data and trends, piping and instrumentation diagrams (P&ID), procedures, alarms, mimics, CAD drawings, etc. are stored in distributed information sources. The plant integration environment allows a single application on the workstation to access these distributed sources and to combine pieces of information from each source into a single application and in this case a single display in that application. This plant integration environment is needed because simply establishing network links among the various systems and information sources, and installing workstations as network nodes addresses only part of the desired support for users.

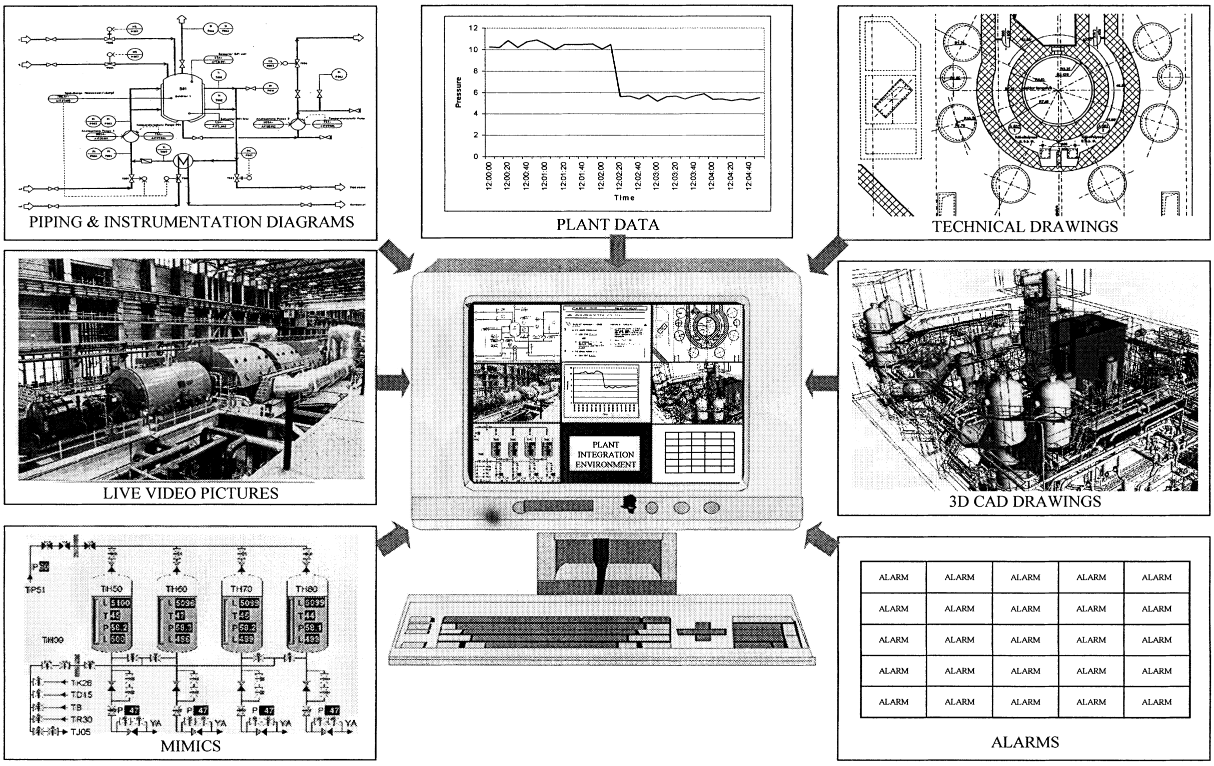

FIG. 5. Integration of plant information.

A common mechanism is needed for transparent access to and interaction with distributed information sources and functionality. Transparent implies plant wide access without requiring the user to become involved in the details of locating and connecting to information sources and functions on the network, interacting with them through diverse transaction mechanisms, and converting information from different sources to a common representation. The environment is also needed to supply the capability to simultaneously access information from different sources and perform multiple functions including information integration. This capability can greatly enhance the ability of the user to integrate information and accomplish his task.

The goal of the plant integration environment is to support the activities of operations, maintenance, engineering, and management personnel at the nuclear power plant and other technical and business offices. This environment provides the needed capabilities that will allow a user to be able to sit at his workstation and gain access to any functionality and information source he requires to do his job, no matter where in the distributed environment of the plant the functions and information reside. At the same time, the integration environment provides access control to prevent unauthorized access to information and functionality. The objectives of this plant integration environment are to:

- Provide a common, consistent interface to I&C systems.
- Enable uniform, transparent access to distributed information sources.
- Establish a computing environment that facilitates the integration of information and applications.

- Furnish a system architecture that permits flexibility in implementation and expandability of functional capabilities.
- Define an approach to application support that lays the foundation for standardizing functions and interface conventions for the plant.

The environment physically consists of workstations distributed throughout the plant and other sites that are connected to the plant communication networks. These workstations are usually made up of conventional computing platforms ranging from personal computers with windowed, multitasking operating systems to high-end engineering workstations. The environment will support a number of software applications, some of which are currently available from suppliers and others that are unique applications which are possible only with shared information and integrated functionality.

The essential elements of the plant integration environment are information access, resource management, control access, human–system interface, and application support. The functional architecture of the plant integration environment provides a layered organization for applications, software services, and hardware components. Each layer provides functional entities to support the accomplishment of plant tasks using the workstations, with the capabilities and services of lower levels supporting the functionality of higher levels. These layers should not be confused with the layers of the communication model. The plant integration environment is an application using the communication model.

To provide the desired functionality with flexibility and expandability, the plant integration environment should be characterized by interoperability, portability, and integration. Interoperability is the characteristic of a system that allows system functional modules and applications to communicate and interact with each other even if they reside on different hardware and software platforms. This is accomplished through well-defined interfaces. These are used to support communication and interaction between the plant systems and information sources and the integration environment. Portability ensures that the applications are de-coupled from the computing hardware and operating systems so that they may be transported from one system to another. Portability is also accomplished to a large part through well-defined interfaces. Integration of both functions and information contributes significantly to the usability of the system. The plant integration environment provides access integration, spatial integration, and function and information integration. These characteristics of the environment are the characteristics of open systems.

An example of this plant integration environment is the Plant-Wide Integrated Environment Distributed on Workstations (Plant-Window) System [8]. The plant-window system concept provides a flexible environment that will accommodate existing applications and computing resources as well as new ones developed under the integration environment. The layers of the plant-window system as illustrated in Fig. 6 are:

(1) Platform applications — this layer includes the existing, non-integrated applications at a plant and the native operating system interface of the workstation platform, these are legacy software applications that do not use the plant-window system function libraries or other integrated services. The need to interface with these platform applications is still quite common. The plant's need for special interfaces to overcome the difficulties of these stand-alone applications is the same as described in Section 4.2.

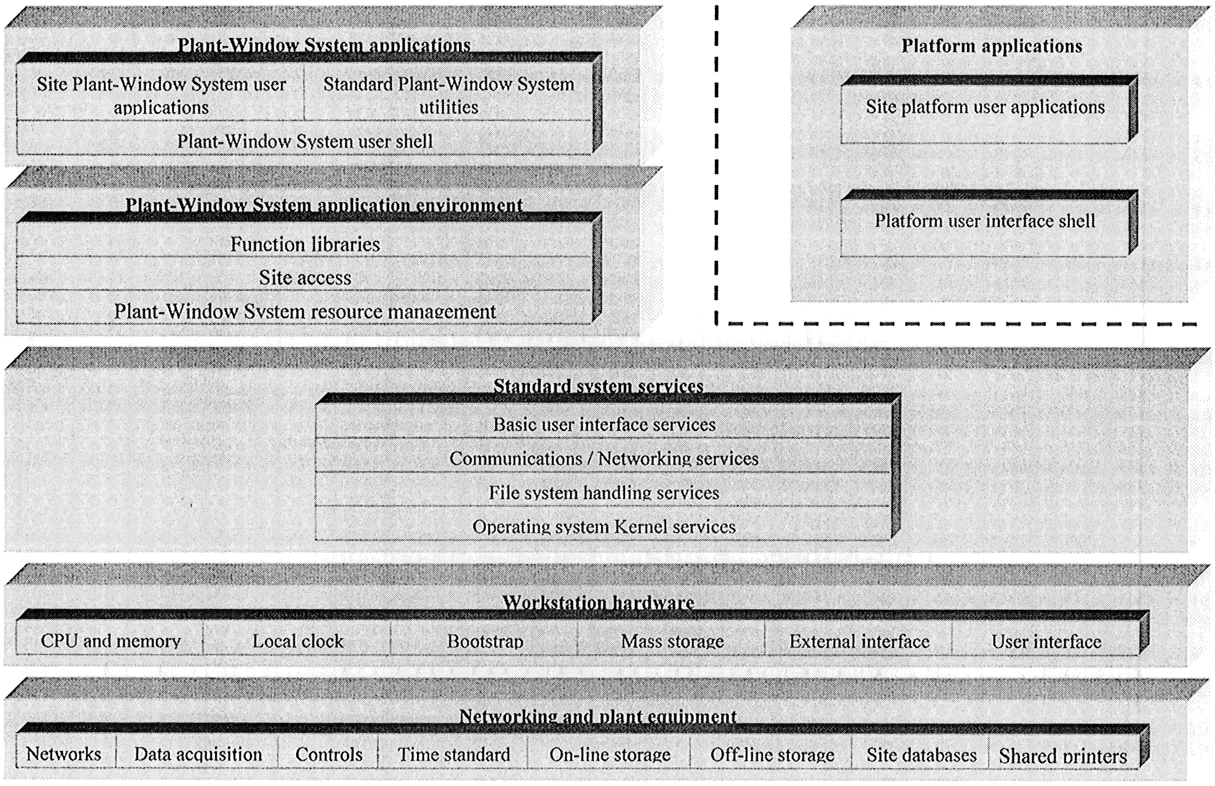
Plant-Window System applications
Site Plant-Window System user applications
Standard Plant-Window System utilities
Plant-Window System user shell
Plant-Window System application environment
Function libraries
Site access
Plant-Window System resource management
Platform applications
Site platform user applications
Platform user interface shell
Standard system services
Basic user interface services
Communications / Networking services
File system handling services
Operating system Kernel services
Workstation hardware
CPU and memory
Local clock
Bootstrap
Mass storage
External interface
User interface
Networking and plant equipment
Networks
Data acquisition
Controls
Time standard
On-line storage
Off-line storage
Site databases
Shared printers

FIG. 6. Plant-window system layers.

(2) Plant-Window System applications — this layer includes user applications that perform plant tasks, standard utilities that provide user access to basic Plant-Window System capabilities, and the user shell that provides the user's interface to the Plant-Window System applications; that is, these are software applications that do use the plant-window system function libraries and other integrated services.

(3) Plant-Window System application environment — this layer provides the application support functionality of the Plant-Window System that facilitates integration. It includes function libraries that provide standard modules to perform tasks for applications, distributed operations for coordinating activities throughout the Plant-Window System, site access services that facilitate integration with plant systems, and resource management that administers Plant-Window System configuration and authorized access to the Plant-Window System capabilities.

(4) Standard system services — this layer includes the basic operating system functions provided by typical engineering workstations. In addition, industry standard distributed computing and communications services are provided. These functions and services provide the core capabilities of workstation platforms. The Plant-Window System environment manages the access and use of these services to give integrated computing support across the distributed Plant-Window System architecture.

(5) Workstation hardware and networking and plant equipment — these layers provide the computing, communications, and I&C equipment that is part of or is connected to the Plant-Window System. The workstation hardware for a Plant-Window System console is configured according to the primary tasks it is intended to support. The network and plant systems depend on the existing plant configuration and the plant infrastructure plan described in Section 4.2.

The plant integration environment concept involves a functional approach for developing a system of workstations to act as common interfaces to plant functions and information. This concept can be adapted by the utility to fit within its existing or planned plant communications and computing configuration and it can support incremental changes between the former and the latter.

5. ANALYSIS OF NEEDS

5.1. INTRODUCTION

In order to size and design the information system and to be able to interact with the plant through the system, each type of user and his needs for information have to be identified. To achieve this, different types of analyses have to be performed. These analyses should preferably start with the identification of the overall goals and main objectives of the plant. With this information as a basis, more and more detailed analyses are performed with the objective to identify each type of user as well as each single task and the support needed to perform each of these tasks.

The objective of performing these analyses is to ensure, as far as possible, that the implemented system or function fulfils not only its specific objectives but also integrates as intended with surrounding functions or systems and that undesired side-effects are avoided. The goal of performing the analysis in the beginning of a project is to thoroughly define the system or function and its capabilities before the system is designed and implemented. This enhances the success of the system and reduces the likelihood of having to make costly corrective actions once the new function or system has been installed.

The result of the analyses performed should be documented in such a way that they can be effectively used in all relevant phases of the specification and design of the system. This implies that the analysis results should be part of the plant documentation. The results of the analyses are also used as the basis for project specific documents and, for this reason, also should be part of the project documentation. The structure of the documentation should allow easy access and use by the staff both for the current project and for other activities.

5.2. THE PROCESS OF PERFORMING ANALYSES

Different types of analyses may be used in different phases during a project life-cycle. In a hierarchical top down approach, analyses are performed on different levels. On the highest level overall goals and main objectives are identified. On subsequent lower levels are these goals and main objectives broken down to more and more detailed specifications at the same time as different types of other inputs and constraints are addressed, e.g. the infrastructure plan. One example of a top down analysis approach is described in IEC 964 [9]. Although this standard focuses on control room design, the principles of performing analyses could be applied for all kinds of system design.

In a top down approach, analyses could be performed on four different levels:

(1) Functional analysis is the first level. The functional analysis should identify the overall goals and main objectives of the plant. The plant overall goals and main objectives are then broken down in order to identify the main objectives and goals for the system.

Besides the goals and objectives, other inputs and constraints important for the more detailed specification have to be identified. The plant infrastructure plan should be identified as one of the important inputs for the more detailed specification. If no plant infrastructure exists, the development of such a plan should be prioritized.

(2) The second level, identification of functions, encompasses the identification of functional design objectives for the system and the human–system interface as well as the identification of any interaction with non-operator users including off-site staff. In order to be able to do this, each type of user of information has to be identified. The plant infrastructure plan facilitates the identification of functional design objectives.

(3) Task analyses are performed at the third level. The task analysis is one of the most important activities during the architecture and basic requirements specification phase. Detailed task analyses are performed with the objective to identify each task to be performed by each type of user. The result of the task analysis together with other inputs and constraints identified earlier (e.g. regulatory requirements, utility policies, the concept of plant design etc.) form the basis for the determination of the level of automation and the distribution of control, i.e. centralized versus local control. The plant infrastructure plan also facilitates the task analysis since it will provide rules and information on how and where information is available and how information shall be distributed.

(4) Detailed analyses, verification and validation (V&V) constitute the fourth level. On this level the design is validated against the functional specification. When a more developed design is available, detailed analyses are performed which could be, for example, the basis for the development of training courses for the staff and the creation of operation and maintenance procedures. The analyses performed at this level are also used to verify the capability of the staff and the systems to perform their assigned tasks. Based on the result of the V&V activities in this level, the long term infrastructure plan should be updated.

The activities described above should be performed in an iterative manner. It should be emphasized that this includes V&V activities**.**

5.3. COMPREHENSIVENESS AND DEPTH OF THE ANALYSES

The comprehensiveness and depth of the analysis to be performed depend on how comprehensive the target project is, i.e. for a new design the scope of analyses has to be larger. In retrofit projects much of the original basic and general analyses can be reused reducing the overall effort. The identification and analysis of design inputs and constraints, as well as carrying out the task analyses are, however, equally important, independent of the size of the project or if it is a new design or a retrofit.

The effort required for the analyses depends also on the importance of the target project as regards to safety and/or plant availability. The cost/benefit of the analyses depends on how important it is to get all the prerequisites correct from the beginning. This should take into account the estimated cost to correct mistakes in the design once the system is taken into operation. Bad solutions and mistakes in the design can to a large extent be avoided if the end-user is involved early in the analysis. Since the level of abstraction is high in the first phases of the life-cycle, when no system exists even on paper, the end-user involvement should increase throughout the design process. Apart from the involvement in the analysis, the end-user participation in the V&V activities is of great importance. The end-users are the best persons to judge if the systems are able to provide the information needed and allow the users to perform their assigned tasks in an optimum way.

5.4. INPUT DATA AND CONSTRAINTS

Requirements and constraints are different depending on if the target project is a new design or a retrofit project. In the case of a new design (a new system), there are fewer constraints since the number of existing solutions to adapt to is usually fewer than in the case of retrofits. A common factor for both types of projects is economy. Overall plant goals and objectives such as keeping the cost as low as possible should be taken into account in the design process as well as when task analyses are performed. Thorough analysis work should make it possible to identify all cases when goals are competing. If these cases are identified early, cost-effective countermeasures could be taken before the design process starts.

The list below contains examples of input requirements and constraints that may have to be taken into account:

- Regulatory authority and licensing requirements.
- Application of standards and rules.
- Costs and cost/benefit analysis, taking into account the entire life-cycle.
- Size of control room staff.
- Size of plant support staff.
- Location of corporate office.
- Existing plant philosophies, for example:
  - long term infrastructure plan.
  - level of automation.
  - use of computers in for example safety applications
  - centralized versus local control.
- Existing plant information systems and their characteristic features.
- Assignment of specific tasks, for example:
  - plant security.
  - fire protection.

It may be the case, that not all information needs are identified when the analyses are performed. Such additional needs for information could be added if enough spare capacity was included from the beginning. Adding spare capacity should be considered during the design phase of the project since information usually represents a higher value than hardware capital costs.

In many cases, especially for larger projects, the cost/benefit of the project, together with specific input requirements and constraints are documented in a feasibility study. In the case of retrofit projects it is also important to identify the advantages, weak points, opportunities, and threats to the existing system and control room design.

5.5. IDENTIFICATION OF THE USERS OF INFORMATION

In relation to a nuclear power plant, different categories of staff are the users of information generated by the plant processes. In order to be able to properly design the I&C system and to determine the number of human interfaces required, each category of users has to be identified. Examples of these users are:

- Control room operators including the shift supervisor and other members of the control room staff.
- Field operators.
- Technical support engineers.
- Physicists and engineers working with core design and evaluation of core performance.
- System engineers and technicians.
- Maintenance staff.
- Chemists.
- Management.
- Emergency center staff (staff in the Technical Support Center).
- Other on-site staff.
- Off-site staff (dispatchers, engineers, management, etc.).

It is recommended to identify the types of users for the specific application in order to achieve conformity between the user and his responsibilities, to identify the sets of data delivered to him, and to identify the data items to be provided or modified by the user. The user should obtain all of the information needed for his job in a useful and usable form. When the user categories have been identified, it is possible to proceed with the analysis of the information needs of each user category. The user should be properly informed about data items and their required accuracy for which the user is responsible, and given the support he needs to maintain the data items, so that other users are supplied with reliable information only.

When each type of user is identified it is also important to perform an analysis to identify the information needs for each category of users. The combined knowledge of information needs and the number of users are then used to determine internal system communication needs, as well as the impact on utilized networks. When the system is implemented it is beneficial to identify the unused capabilities of the new system. The unused capabilities should either be removed or prohibited from use.

6. MAPPING THE SYSTEMATIC APPROACH TO A SYSTEM LIFE-CYCLE

6.1. INTRODUCTION

All of the phases of a computer system or function, from the conceptual idea to the end of its useful lifetime, could be described as the system or computer function life-cycle. Typical life-cycle phases are: feasibility study, requirements specification, tender specification, purchasing, system realization, implementation, operation and maintenance. Each phase of the life-cycle should be defined and requires a formal set of input documents that provides all guidance, information and constraints needed in order to perform the activity within the phase. The activity performed will create another set of documents providing evidence that the activity is completed and that the product, which is the output from the phase, meets the input requirements.

Guidance on the contents and phases of a reference life-cycle is found in standards, such as IEC 61508 [10], and IEC 880 and its supplement [11] as well as in the IAEA QA manual for computer software [12]. Guidance on what documents are required as input information or generated as the result of activities within a specific life-cycle phase is found in Ref. [13].

Depending on the complexity and importance to safety of the system, there is a spectrum of documents needed as input for each phase of the life-cycle. From information integration point-of-view, the plant infrastructure plan, together with the results from the analyses of needs, are particularly important. The infrastructure plan and the result of the analyses should be considered throughout the whole life of a system or a function, but they are especially important at the following phases of the life-cycle:

- Project initiation and identification of goals and constraints.
- Project preparation and feasibility study.
- Architecture and basic requirements specification.
- Tender specification.
- Specification of individual systems.
- System realization.
- Implementation, operation and maintenance.

The way the systematic approach to information integration, i.e. long term planning, the infrastructure plan and the analyses of needs, is mapped to each of the above listed phases in the life-cycle, is described in more detail in the following text. The life-cycle phases listed below follow the phases identified in IAEA-TECDOC-1066 [13]. A life-cycle model based on that document can be seen in Fig. 7 (a, b). The life-cycle in the figure is simplified but the steps that are important to information integration are highlighted.

Verification activities shall be performed throughout the entire life-cycle. A verification activity should be conducted at the end of each project phase. A successful result of it is a prerequisite for the initiation of the next phase. A validation of the entire system shall be done in order to demonstrate the compliance with the requirements specification. Guidelines for the performance of V&V activities is provided in an IAEA technical report [14]. A special case is the V&V of the human–system interface, where it is often seen that this activity comes at the very end of the project when it is too late or too expensive to make changes. The advocated approach is to perform HSI V&V from the very beginning of the project by establishing independent review teams and performing incremental V&V at each phase of the system development. This will avoid the need and added expense for making large changes at the later stages of the project.

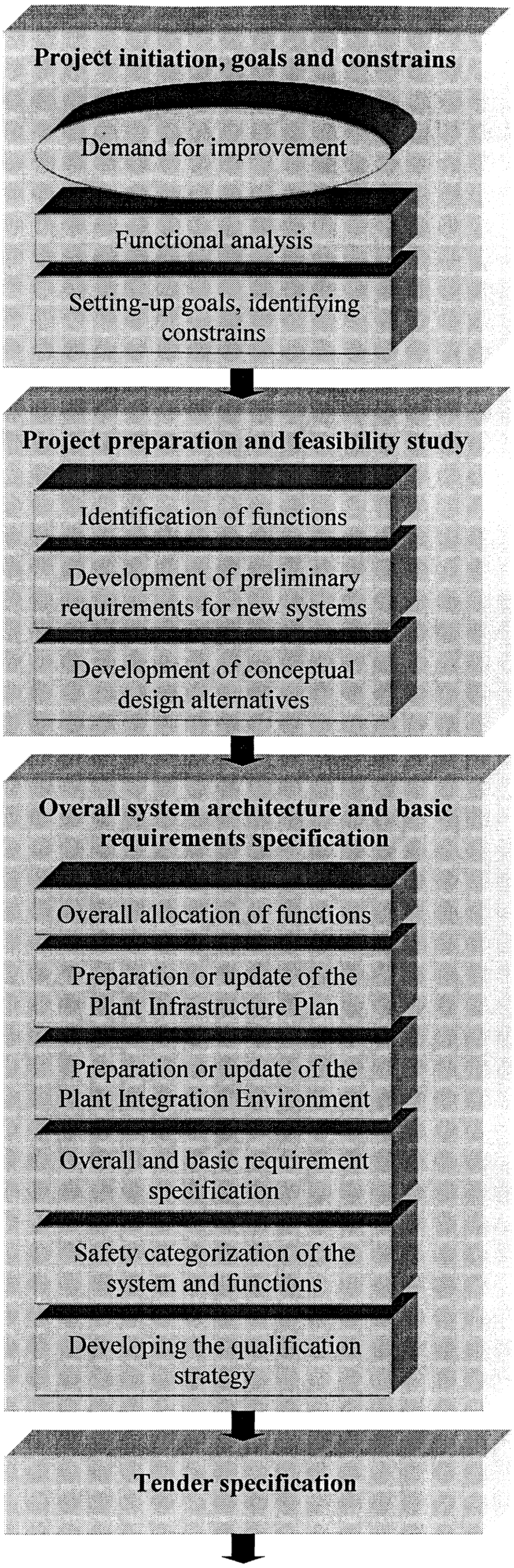
Project initiation, goals and constrains
Demand for improvement
Functional analysis
Setting-up goals, identifying constrains
Project preparation and feasibility study
Identification of functions
Development of preliminary requirements for new systems
Development of conceptual design alternatives
Overall system architecture and basic requirements specification
Overall allocation of functions
Preparation or update of the Plant Infrastructure Plan
Preparation or update of the Plant Integration Environment
Overall and basic requirement specification
Safety categorization of the system and functions
Developing the qualification strategy
Tender specification

FIG. 7 (a). Life-cycle model of information integration.

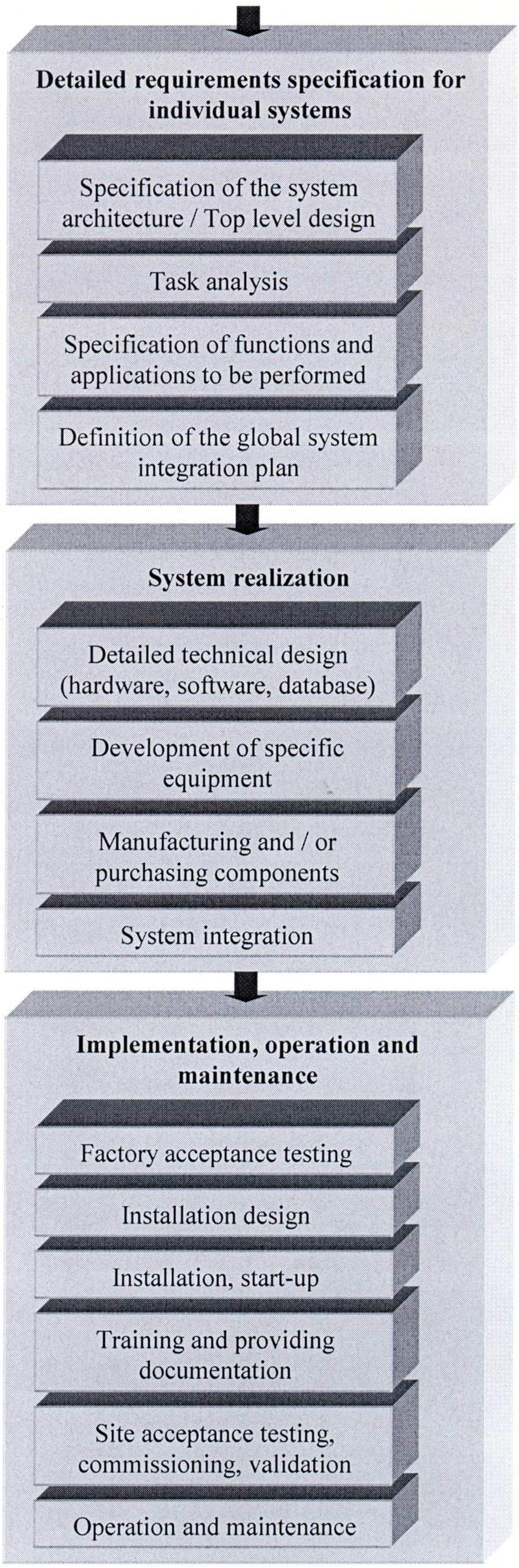
Detailed requirements specification for individual systems
Specification of the system architecture / Top level design
Task analysis
Specification of functions and applications to be performed
Definition of the global system integration plan
System realization
Detailed technical design (hardware, software, database)
Development of specific equipment
Manufacturing and / or purchasing components
System integration
Implementation, operation and maintenance
Factory acceptance testing
Installation design
Installation, start-up
Training and providing documentation
Site acceptance testing, commissioning, validation
Operation and maintenance

FIG. 7 (b). Life-cycle model of information integration.

6.2. PROJECT INITIATION, GOALS, AND CONSTRAINTS

When demands for improvements are identified, specific goals should be set up and the application domain and constraints for the project should be identified. Functional analysis could be used as a method in order to identify a hierarchy of goals as well as the limitations and application domain for the project. It is recommended to take into account the needs of and constraints on information integration at this early stage by mapping the project to the long term plant infrastructure plan.

6.3. PROJECT PREPARATION AND FEASIBILITY STUDY

The main activity of this phase is the production and reporting of the feasibility study. Some of the activities important to information integration are:

- Review of the present I&C systems requirements documentation (or developing it if not available) as input information for consideration to new systems.
- Review of the long term plant infrastructure plan (or developing it if not available) as a prerequisite for the new system.
- Identification of the functions and associated systems, as well as equipment belonging to the scope of the system.
- Identification of weaknesses and strengths of existing systems in their functionality, performance, dependability, operability, integration with other systems, and other key features.
- Development of preliminary requirements for new systems, with special attention to requirements that expand beyond those of the existing systems.
- Development of conceptual design alternatives for the new system.
- Identification of the benefits of safety and operation expected.
- Development of cost estimates for new system alternatives over the expected life time of the system and making a comparison of cost/benefits for new system alternatives.
- Selection of the optimum conceptual design for the new system.

6.4. ARCHITECTURE AND BASIC REQUIREMENTS SPECIFICATION

The main activities in this phase are the development of design concepts and the development of a basic or overall requirements specification. Some of the activities important to information integration are:

- Overall allocation of functions and tasks.
- Specification of the overall system architecture, showing the systems and interconnections impacted by the project and an outline of the scope of the project.
- Specification of overall and basic requirements for functionality, performance and dependability for the different functions including information integration.

- Identification of the safety relevance of the system and categorization of the system and functions important to safety.
- Development of the qualification strategy for the integrated system.

With regard to information integration, one of the most important activities in this phase is the development of a project specific infrastructure plan to support communications and computing. This infrastructure plan should be consistent with the long term plant infrastructure plan mentioned in Sections 3.2 and 4.2 above.

The plant specific infrastructure plan should support the acquisition, storage, access, computation, and display of the required information. The computer and software architecture should be made reliable and robust to handle possible hazards or errors that may occur. Sufficient redundancy, diversity, and data validation should be built into the system. This becomes even more important when multiple users make decisions based on common shared integrated information.

Another important activity related to information integration is the development of a plant integration environment. This environment is developed after the infrastructure plan is created. It consists of a set of requirements that will provide a common, consistent, and easy to use interface to distributed information and functionality. It will also provide the tools to support uniform human–system interfaces to display information in a usable and useful manner. It will provide a foundation for standardizing functions and interface modules to make them easier to use. A major characteristic of both the infrastructure and this environment should be that they are adaptable, flexible and expandable to meet future as well as current requirements, including safety requirements. Basing them on open systems standards is essential to support this requirement and to allow the interoperability of functions. This will also allow portability by de-coupling the information and functionality from computer hardware and communications network details.

The infrastructure and the environment should also support the integrity of the information. For example, it is important that a non-safety system or function cannot corrupt information for a safety system or function. Similarly, information for a process control system or function should not be able to be corrupted by an information system or function. Yet, it is important that information from safety systems, process control systems, and information systems is available to the appropriate users, and to display and storage devices. This can be achieved with the proper configuration of networks and one-way links between them.

The preparation of the plant infrastructure plan and the plant integration environment has been discussed in detail in Section 4.

6.5. TENDER SPECIFICATION

The main activities are the suppliers' initial development of designs, time-scales and quotations. This phase does not encompass any activities that are specific to the information integration except to ensure that the required information integration and overall human–system interface (HSI) requirements are accommodated by the proposed design. The tender specification phase utilizes the work performed in the previous phase in order to make it possible to select a supplier.

6.6. SPECIFICATION OF INDIVIDUAL SYSTEMS

The main activity of this phase is the production of the individual system specification and software requirements. This phase is completed by functional validation. The validation concerns only the specified functionality to ensure that the following phases of the system realization are not subject to expensive reworks due to missed functionality. Some of the activities important to information integration are:

- Specification of the system architecture.
- Specification of the functions and applications to be performed based on task analyses.
- Definition of a global system integration plan.

The specification of the functions and applications need to be compatible with, and should take advantage of the integrated infrastructure and environment. An integral part of the specification activity is to identify the planned users of the applications, the type of use they plan to make of the application (this could vary with different sets of users), the sources of information that are required for the application, the required presentation of the information and results (this too can vary with different user groups), and the possible locations of the potential user groups. The most important tools to perform this activity are task analyses.

It is important to involve the identified users when the task analyses are performed and the detailed specifications are written. The purpose is to obtain their involvement in the design of the application, especially with the human–system interface, to help ensure the usability and usefulness of the application. The ability to easily address the needs of various groups in various locations is facilitated by the integrated infrastructure and environment.

Task analyses are described in a more detailed manner in Section 8.6.

6.7. SYSTEM REALIZATION

The system realization phase consists of detailed specification of the software and hardware; as well as coding, manufacturing, and integration of the hardware and software into a complete system. Some of the activities important to information integration in this phase are:

- Preparation of detailed system design.
- Software design, implementation, and testing.
- Database design and implementation.
- Hardware design, manufacturing, and testing including the human–system interface.
- Development of specific equipment (e.g. interfaces to other systems).
- Purchasing and manufacturing of standard components and modules.
- Integration of hardware and software according to the integration plan.
- Integration of hardware and software for the factory acceptance testing.

During the detailed design, special attention should be paid to the ergonomics of the HSI, data security, and the design of the alarm functions as discussed in Section 7.

6.8. IMPLEMENTATION, OPERATION AND MAINTENANCE

Although information integration activities belong to the phases that come before the implementation of the individual systems, feedback from the implementation phases is essential in order to provide input and lessons learned for new projects. The main phases in the implementation of the system are:

- Factory acceptance test.
- Installation and preparation for operation of the individual systems.
- Training and writing final documentation.
- Site acceptance testing and commissioning in the plant.
- System operation and maintenance.

Adequate procedures should be established for system maintenance and updates of the system components (software, hardware, and information) to avoid introduction of errors after system installation. The end-users should be informed about changes that may have an influence on their applications and information sources.

7. IMPORTANT ISSUES FOR INFORMATION INTEGRATION

7.1. INTRODUCTION

Besides the topics discussed above, there are other important issues related to information integration, such as human–system interfaces, the special requirements for alarm handling, and data security. These are described in Sections 7.2 and 7.4.

7.2. HUMAN–SYSTEM INTERFACE

The human–system interface should be designed such that the operators are always aware of the actual state of the plant and are never exposed to information overflow, even in the case of the worst plant disturbances. The human–system interfaces should have a consistent look-and-feel in order to reduce the likelihood of confusion, misoperation, and misinterpretation.

The ultimate goal of the human–system interface is to provide better information presentation, which combines information from different sources, performs data processing and prioritizes and highlights information essential to plant personnel. For this to happen, the design needs to properly account for the role of humans in using and maintaining the systems. End-user involvement in the whole life-cycle is essential.

7.2.1. Major concerns

The operators use human–system interfaces and other electronic and written tools to perform their tasks. If the HSI and the other operating tools are not well integrated or are inconsistent, this can cause inefficiencies and errors. In order to assure adequate integration and consistency, it is necessary to develop both the HSI and the supporting tools in a consistent manner.

Another concern is to design efficient navigation functions in large display systems consisting of several hundred pictures. This could be resolved by properly designed display hierarchies, the use of dynamic function buttons, context-sensitive menu systems, etc.

The effect a new information system has on the team performance is also important. A set of design and implementation guidelines should be developed for human–system interfaces, and should be used for all new applications to ensure consistency. Users should be involved in the entire design and implementation process, including V&V, to ensure that all aspects of operation and user needs are covered and handled properly.

Other concerns when introducing new information systems into an operating nuclear power plant is the ability of humans to adapt to the new technology and to operate with mixed technologies while preserving a high safety standard. Questions like the ones below may need to be answered:

- Is the information presented at a sufficiently high level of aggregation to support the decision-maker?
- Does the information integration and extraction impose additional work or cognitive burdens for the end-users?
- Are the displays readable and the information readily accessible?
- Is the information presentation and retrieval consistent across the systems?

7.2.2. Human–system interface plan

In order to identify and manage all aspects of an I&C change that has an impact on humans, a human–system interface plan should be established. This plan should be available before the specific project starts. The need for the human–system interface plan is identified in the IAEA Safety Reports Series No. 6 [2]. Guidance for developing such a plan can be found in Ref. [15].

7.2.3. HSI function and task allocation

The new technology offers many possibilities for automating information processing (also known as “soft automation”, e.g. alarm analysis, computerized procedures, sequence control, and more advanced process control features. When designing the HSI it is important to maintain human consciousness about what the computer/automation system performs and what manual actions are needed by the human to stay within the “loop” and understand the situation. Such a design is also referred to as “human-centered automation” [16].

This division of automated and manual tasks is addressed in the analysis phase (see Section 5. However, it is difficult to identify all the user needs before the design stage begins and the complexity of certain tasks is determined. Therefore, the division of the tasks should be addressed in the design process when the different pieces of information are put together. This is the time to verify if the user is capable of comprehending all of the available information and, at the same time, maintain the overview of the situation.

7.2.4. User involvement in the HSI design

The HSI design process has to identify all user categories affected by the scope of the design, satisfy the user needs, and identify interfaces to other HSIs to make sure that there is no adverse effect on them.

It is advisable to establish an HSI group in order to prepare the human–system interface plan, to keep control on HSI modifications, to assist the execution of the HSI portion of I&C projects, etc. This group should represent all categories of end-users and include a human factors specialist. The group should participate in all phases of the I&C project.

The end-users' viewpoints should be documented and used as part of the requirement specification for the HSI. This will facilitate the satisfaction of users' needs in the HSI design and help achieve user acceptance.

7.2.5. Design considerations for the HSI

The HSI design should follow a "top-down" approach when considering the shift crew working as a coordinated team and a "bottom-up" approach when considering the individual work positions. For teamwork, all necessary information should be available to all crew members simultaneously, and communication within the team should be supported. As emphasized earlier, the workplace for the individual crew member should be determined based on a thorough task analysis.

In addition to the specific needs of each individual user, it is also necessary to ensure information sharing amongst teams and control room crews. The work situations in the control room may change rapidly, depending on the process behavior. The control room and user interface should be suited for both a relatively static monitoring condition with a stable plant state, and a rapidly changing situation with increased workload. All plant states should be considered when designing the HSI.

The technical staff outside the MCR represent a variety of user categories with different tasks and responsibilities. Consequently, the information needs may vary substantially as specific tasks arise. Therefore, the HSI should be designed to be flexible to allow possible changes after installation.

Frequently it is desirable to use existing, specific application software or commercial-off-the-shelf software/hardware products for modernization of a system. These existing and COTS products will normally not perfectly satisfy the users' HSI requirements. Therefore, it is important to adhere to the HSI plan during discussion with the supplier to develop a set of acceptable requirements to the user, which can be satisfied by using the existing or COTS product. If it is not possible to adhere to the HSI plan, then it is suggested that the proposed product should not be used.

Another area of concern is that the suppliers of COTS products are likely to continue to modify their product for commercial reasons. In order to assure that the new versions will still satisfy the requirements, the supplier should have a configuration management process in place that is adequate to allow the user to determine the changes made to the product. This will allow the user to determine if the new version still satisfies the requirements.

7.2.6. Human factors and ergonomics

There are a number of human factors issues that need to be addressed when making changes in the information presentation and redesigning the HSI:

(1) The role of the operator and other users should be analyzed. The operator functions may change in character from traditional process monitoring and control to a more supervisory role, which also involves more planning and administrative work.

(2) Increased automation, e.g. automatic control, computerized surveillance functions, may replace parts of the manual work. Further, new advanced operator support systems may be introduced. This may require more education, training and qualification of the personnel.

Changing from conventional instrumentation presentation to more VDU-based information presentation and control influences several factors:

(1) The operators spend more time in front of the display screens and it is important to design the working environment, e.g. ergonomics, illumination, etc. to avoid fatigue and thereby optimize operator performance and productivity.

(2) If not properly designed, team communication can be degraded because sharing of information is not as easy when each operator is sitting in front of his own display screen. In pure conventional control rooms, the location of the instruments and the control panels that the operators are using are continuously visible and can be seen by other team members. Arrangements of workplaces, display screens, and instrument panels should support team communication and sharing of information. To ensure such support, team communication should be carefully observed in the current control room configuration. In addition, input should be sought from control room crews with respect to their concerns about communication patterns and potential changes and burdens resulting from changes to screen-based displays.

(3) Hybrid solutions should be considered carefully. If information is presented on screens and conventional panels, consistency should be maintained to avoid misinterpretation. If this is not accounted for, additional cognitive burden may be imposed on the operator. Further, control devices and associated information presentation should be closely located to avoid unnecessary movements, e.g. alarm presentation and acknowledgement of alarms.

Further guidance for human factors and ergonomics design can be found in Refs [10, 15, 17].

7.2.7. Transparent access to functions and data

One problem often encountered is that users have to move back and forth between different systems when performing a job or a task. In the past this was mainly caused by limitations imposed by the technology, which made data and functions inaccessible across strict borders of a specific vendor's system. The data exchange format was incompatible. If the user wanted to transfer data, cumbersome translation procedures had to be applied. However, the same problem may occur in the new systems as well. This will happen if integration issues are not carefully considered and previsions are not made to accommodate data exchange and integration. The major pitfalls are the following**:**

- Since modernization is done in an incremental manner in separate projects, the coordination maybe lost or forgotten when it comes to the HSI.
- New I&C modernization projects tend to be very technology oriented and focus heavily on the specific equipment and hardware to be installed, putting less weight on how the plant personnel should be able to operate and maintain the new system together with all the other systems at hand.
- Different vendors may still deliver different functions and systems to the plant and if not stated and specified explicitly in the requirements, most probably the HSI will be different across systems.

New network technology offers possibilities for transparent sharing of data and functions. Careful consideration has to be given to the data security (see Section 7.4). However, as long as safety and security are not compromised, the following rules should apply:

- There should not be any unnecessary restrictions to the access of data plant-wide.
- Information exchange protocols should be standardized to avoid incompatible formats and interpretation problems.
- The user should be allowed to combine information from any information source transparently to meet his specific needs without having to move across systems with cumbersome access procedures.
- The information should be available at different processing levels, e.g. single data vs. aggregated data; raw data, short term history, cycle history, etc.
- Standard processing units or functions (e.g. alarm handling, event recording) should be done in one place and made available to all of the users.
- It should be possible to configure the HSI with a selected set of data, processed data and functions according to the preference of the user.

7.2.8. Data validation

Data validation becomes particularly important in an integrated environment where the same data is used in many functions supporting different tasks and decision-makers. The following rules should apply:

- Data validation should be performed as close to the source as possible.
- Different validation techniques should be applied and explored as far as possible (e.g. single sensor validation, redundancy check, diverse sensors, analytic redundancy, etc.).
- It should be possible to access the raw sensor data if needed for specific analysis purposes (e.g. transient and noise analyses, etc.).

7.2.9. Processing data to match user tasks

Many I&C systems provide and present the data in a very “system oriented” way. This means that the end-user has to “dig” for information in large display hierarchies that are typically organized according to plant topologies. This may be well suited for system maintenance personnel performing diagnosis on the detailed equipment at hand. However, this may be very inconvenient for MCR operators in plant upset conditions, where critical functions need to be monitored.

Data should be processed and aggregated to the right information level for the user. Information hierarchies are needed, but they should be developed commensurate with the navigation complexity, how difficult it is for the user to access information, and the necessity to keep the overview. By providing more integrated displays, the user may be able to maintain the overview of the plant more easily. The same applies to a decision support system (e.g. maintenance support system) which may consist of many detailed displays. Application of overview displays should be encouraged to ease the introduction and use of specific systems.

Task oriented information presentation should be supported and encouraged in the HSI design. This will reduce the need for extensive information search by the end-user and will increase productivity. Important information to support such an HSI design is obtained from the detailed task-analysis performed already in the analysis phase. An example of task oriented information presentation is the use of large overview screens in the control room.

7.2.9.1. Large overview screens

New technology has enabled the introduction of large overview screens. The main features and benefits of these screens are:

- They act as a “reference”, common to all of the control room staff, providing a representation of the whole process. Rapid assessment of the current plant state is supported. As such, they support planning, monitoring, and the shift changeover process.
- They promote group communication, coordination, and situation awareness. They provide a means to inform everyone about actions taken by other crew members. A common understanding is developed. They may serve as a focal point in crew decision making, particularly in stress situations.
- They may serve as the entry point into the hierarchy of display formats. Although physically separated, they are logically connected with the detailed displays. Thus they can support the operator when he has to decide on the selection of specific detailed displays.
- Overview displays are particularly crucial in a “cockpit-type” control room with little conventionally displayed information and where information is accessed sequentially on a limited number of detailed displays.
- They can integrate information from different sources in a clear, consistent, and uniform way rather than self-standing independent displays for each control room system.
- Part of the overview information should be in a fixed location with the same type of information presented independent of plant state.

- The new technology offers the possibility to present context dependent information and to provide a good picture of the plant state both in normal and abnormal situations.

7.2.10. Providing support for user needs

In many cases, the same system provides information to different personnel categories that apply it for different purposes. Examples can be core surveillance, where the operator uses information related to the real-time monitoring of safe operation of the reactor core, while the reactor physicist follows cycle trends and performs predictive simulations. To avoid overloading the operator with a lot of unnecessary information, the HSI of the operator should be tailor made for his needs and use of the system, while the reactor physicists should have all system functions available to them. Consequently, it is necessary to define the knowledge level and identify what is the appropriate support level for the user to carry out certain tasks.

In the future it is envisaged that more operator support systems will be introduced to enhance safety and the performance of NPP operation. This means that new operator support systems should be designed in such a way that they are capable of being integrated with other systems in a unified HSI.

7.3. ALARMS

Alarm systems often cause problems when the operating state deviates from normal conditions. For example, information overload of the operators can occur if too many alarm messages are generated during transients. Modern technology provides means to overcome these problems by adapting the alarm system to different plant states by various alarm processing techniques. Since many upgrade projects are done incrementally over several outages, it is important that alarms from different systems are integrated in a unified manner with a common alarm philosophy as each new system is modernized.

7.3.1. Identified problems and potentials for improvement

Improvement of the alarm system has been identified as one of the most important requirements in modernization projects. The problems identified are:

- Existing alarm systems are usually optimized if they are optimized at all, for full power operation, and could be improved in other plant operating states: during power changes, start-up, low-power operation, outage periods, and disturbance situations.
- Too many alarms are usually presented during large disturbance situations.
- Multiple disturbances are difficult to detect.
- Acknowledgement of many alarms is sometimes a time consuming task.
- Alarms are not presented at the location where the related object maneuvering control takes place.

With an integrated information capability, it is possible to provide a flexible alarm system, which can offer enhanced functions for alarm generation, alarm structuring, and alarm presentation for all users.

The alarm system should be configurable. It should, for example, be:

- Easy to make changes.
- Possible to combine pieces of information from different data sources.
- Easy to build new alarm structures and alarm logic to support the different users in the organization.

7.3.2. Overall requirements

The alarm system is one of the most important information systems in the MCR. For all possible process situations, alarms should:

- Alert the operator to the fact that a system or process deviation exists.
- Inform the operator about the priority and nature of the deviation.
- Guide the operator's initial response to the deviation.
- Confirm, in a timely manner, whether the operator's response corrected the deviation.

In an integrated environment, information is routed to different users outside the MCR, where critical decisions can be made as well. This means that the same overall requirements apply to all workplaces in the distributed system.

The alarm system should be optimized with respect to these overall requirements and adapted to the capabilities and limitations of humans for information handling, problem solving, and decision making.

7.3.3. Overall design principles

The following are the overall design principles for alarm systems:

(1) The "dark screen" principle is important for obtaining an alarm system that only calls the operator's attention when something is wrong. This should be the main principle when designing the alarm system. No alarms should be presented when a process part is in a normal state without failures. During normal changes of the process, a number of parameters are changing. As long as the variations are normal with respect to the state of the process, no alarms should be presented. The main goal is to avoid information overload and unnecessary distractions in all states of the process.

(2) The presentation of alarms should comply with the overall principles defined for the MCR information system and the other workplaces defined.

(3) Alarms should be readable from a reasonable distance in the MCR. If overview alarms are used, it should be possible to identify them from all locations in the MCR.

(4) The alarm system should provide direct guidance to the spatial location of the process section, plant system, etc. in alarmed condition. This can be done, for instance, by a direct reference in a text message for accessing the right format.

(5) Conventional and screen-based alarms should be presented consistently.

(6) Alarm acknowledgement should be possible from all locations where alarms are presented. It should be possible to acknowledge alarms in process pictures, alarm lists and from control panels. Acknowledgement should only be performed once for each alarm, even if it is presented at several places. All operators who have access to the alarms should be able to acknowledge the ones pertinent to their process systems.

7.3.3.1. Alarm structuring

The objectives of alarm structuring are:

- To keep the number of presented alarms at a level where cognitive overload of the operator is avoided in all operational plant states.
- To remove false alarms or alarms with less important consequences.
- To prepare alarm lists for distribution to different user categories.
- To satisfy the operators' need for flexibility, to choose among pre-defined alarm structures and to provide the operators with the capability for searching for adequate data as additional support during plant state identification.

The following three methods should be available for alarm structuring in the alarm system:

- Alarm prioritization.
- Alarm suppression.
- Alarm filtering.

In order to perform efficient alarm structuring, the alarm system should have access to all relevant information sources in the integrated environment in order to make it possible to perform alarm processing.

7.3.3.2. Alarm presentation

Overall presentation principles in the MCR:

(1) Alarm and process information should be integrated. When alarm information is integrated with process information in the same displays, the operator doesn't have to extract information from separate sources to obtain a mental model of the process. This reduces the data acquisition task, as well as the required mental processing effort, for the operator. The interaction workload with the user-interface is reduced, (e.g. use of keyboard, tracker-ball, and exchange of displays).

(2) Alarms should be presented at several levels. With reference to the "dark screen" principle and the principles for filtering and suppression of all irrelevant alarms, the alarm presentation has the following levels:

- At the top-level, all important alarms are integrated with the continuous overview information for the whole MCR.
- The next level should present all alarms that are not filtered or suppressed in one or several alarm overview displays at the operator workplaces (e.g. reactor operator, turbine operator, etc.).

- The third level contains alarms in selective lists and process displays. The selective alarm lists contain all alarms including the suppressed alarms, while the process displays contain alarm information integrated with the detailed mimic diagrams in the MCR.

Alarm systems are usually not causing large difficulties outside the MCR. Those user categories are not in the frontline of operation and have more time to respond and take actions. Nevertheless, for safety and consistency reasons, the personnel in the technical support centers and emergency operation centers have basically the same needs for well-structured alarm information, as do operators in the MCR. People in technical offices and the maintenance staff should obtain relevant and timely information from the alarm system to efficiently carry out their duties. This may save time, reduce personnel costs and as a consequence lead to economical benefits for the utility.

7.3.4. Alarm integration in a hybrid environment

Most nuclear power plants have a conventional control room with analog instrumentation and alarm presentation. Considering that most utilities follow a stepwise modernization program, this means that computerized alarm systems will be integrated in a hybrid environment and will remain so for a long period of time.

The overall principles outlined in the previous sections should apply also to the hybrid solution. This will ensure a smooth transition from a conventional to a fully computerized environment. However, there are certain important areas to pay particular attention to when combining conventional and digital alarm systems:

- Alarm presentation should be consistent across conventional and screen-based systems, i.e. use of alarm symbols, text, colors, etc.
- Annunciation principles should be consistent and in accordance with selected prioritization schemes, i.e. color coding, blink frequencies, sound tones and levels, etc.
- Acknowledgement principles should be consistent, and acknowledgement should be possible to be performed from either system.
- The computerized system should provide an interface with analog instrumentation and data and alarm information to ensure that consistency is preserved.

Nevertheless, these restrictions or constraints should not hinder the designers from taking benefit of all of the advantages provided by computerized alarm systems. Especially, the ability to combine information from different sources should be explored and encouraged in order to perform alarm structuring that matches the users needs and capabilities.

7.3.5. Plant wide alarm integration

Traditionally, alarms are generated from individual sensors leading to the classical one-sensor/one-indicator solution. This approach suffers from several problems such as:

- Many alarms are generated during transients.
- Many non-relevant alarms are issued when the plant is in another state than the main mode of operational, e.g. during outage periods, etc.
- The information content derives from a single alarm source, which means that the user has limited help from the alarm system in many situations.

An integrated information environment offers new possibilities for enhancing the alarm systems. Data can be combined from different sources and processed to obtain higher information content than can be achieved with single sensor data. Examples of such processing are:

- Critical function alarms important to monitoring the status of critical plant conditions as used in symptom based emergency operating procedures.
- Pattern matching techniques to recognize alarm patterns of important transients and events.
- Suppression of irrelevant alarms in transients and different system states and plant states.
- Utilization of combinations of diverse instrumentation to give early warnings to indicate possible problems and consequently to be able to take countermeasures in advance of events that could occur.

When designing the new integrated information system, it is important to look carefully through the system architecture (see Section 4) to ensure that all data needed for creating an integrated alarm system is provided. Some industrial systems tend to impose restrictions on access to basic alarm information. This makes it difficult to implement an integrated alarm system fulfilling the requirements for flexible structuring and processing as described above.

Considerable research has been done on development of improved alarm processing methods, and new tools are provided [18].

An interesting, new approach for alarm systems has been introduced in Beznau where significant improvement in alarm processing has been reported [19].

7.4. DATA SECURITY

Information is a valuable asset and in many cases the safe operation of a nuclear power plant relies on the availability, correctness and timeliness of information. Due to this, the information as well as the information storage devices and the media carrying the information have to be protected and the access to information has to be restricted. It is also important to take into account the possibility that there could be malicious attempts to destroy, disturb, or corrupt information. In order to achieve a balanced level of protection, taking into account all types of threats, different types of security measures have to be implemented. The security measures could be both administrative and physical. The potential interactions between factors that affect data security risks are graphically depicted in Fig. 8.

Physical protection of data encompasses, e.g. physical access control, fire protection, reliable power sources and reliable cooling and ventilation.

Data security also comprises the protection of information belonging to safety functions. I&C functions are categorized according to their importance to safety. Functions belonging to a lower safety category must not be able to disturb or interfere with functions belonging to a higher safety category.

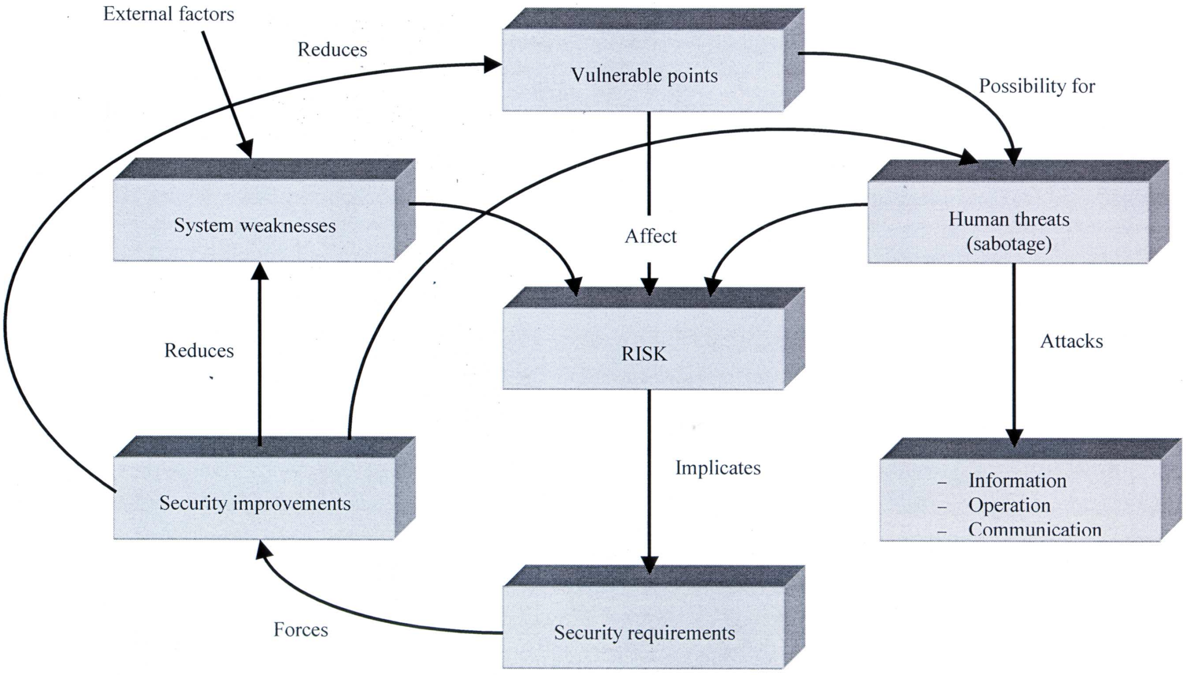

FIG. 8. Interaction between factors that affect data security risks.

Another important data security aspect is to ensure information back-up and recovery after failures. It is recommended to have a data security policy on a plant level as guidance. The data security policy should be taken into consideration when the plant information plan and plant information environment are produced.

7.4.1. Plant data security policy

The security policy should contain clear and unambiguous goals and guidance for how these goals should be reached. Beside goals, the data security policy should contain general rules about how information shall be managed and how information is accessed.

The data security policy should be in compliance with the plant security policy if such a policy exists. In order to keep the data policy up-to-date, it should be reviewed regularly (see Fig. 9). Listed below are some items that may be included in the plant data security policy:

- Data security goals.
- Legislative and regulatory requirements.
- Reference to the plant security plan.
- Identification of threats against the plant information environment.
- Reference to the plant information plan.
- General rules and guidance on data security.
- Responsibilities.
- General rules on data back-up activities.
- Information recovery plan.
- Definitions.

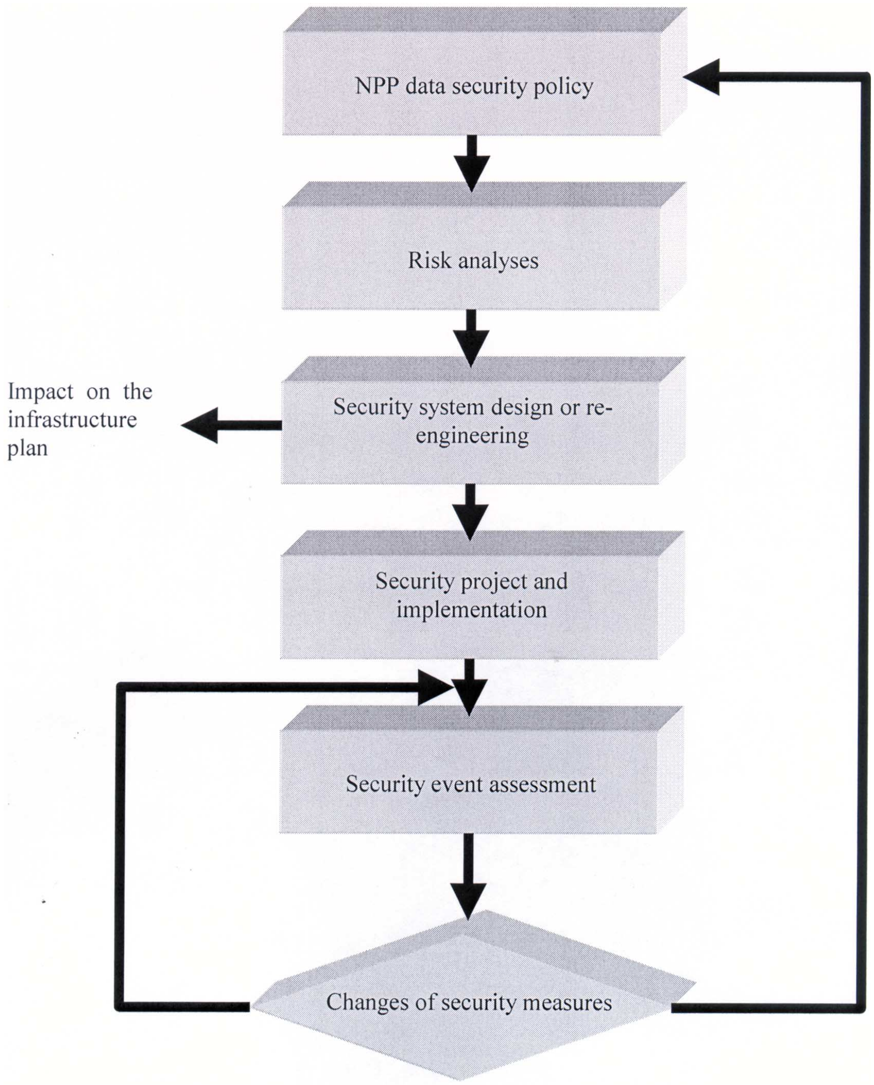
NPP data security policy
Risk analyses
Impact on the infrastructure plan
Security system design or re-engineering
Security project and implementation
Security event assessment
Changes of security measures

FIG. 9. Process of performing data security risk analyses and its effects on the data securiiity policy.

Possible data security goals, which could be used as a basis for quality assurance criteria for data and information, are:

- Consistency — data and information are maintained in such a manner that they are free from contradictions.
- Accuracy — correct data and information conforms to plant requirements and standards.
- Timeliness — data and information are provided to their user at the time required or specified.
- Validity — the quality of data and information is found rigorous enough to achieve acceptance.
- Relevancy — the state of data and information corresponds with user's needs and user's knowledge.

- Reliability — the quality of data and information that permits them to be rationally correlated with other similar data or information.
- Stability — the ability of data and information to satisfy additional or changing requirements over time without affecting the original design.
- Extensibility — the ability to accommodate additional values of data without affecting the original design.
- Flexibility and/or modularity — the ability of data and information to accommodate requirements of change without reengineering of data structures or other major components of the design.

7.4.2. Responsibility for data security

In order to clarify who is responsible for the integrity, availability, and validity of each data element, a responsible person or a responsible organizational entity should be identified. The responsible person or the organizational entity will act as the owner of the information. The person's or entity's responsibility is to:

- Classify information according to some attributes, for example, the plant data security policy.
- Validate the correctness of the information.
- Assure information availability according to requirements set up for each information element or group of elements.
- Grant access to the information and provide rules and restrictions on how the information can be used.
- Apply the data security policy rules appropriately.

7.4.3. Classification

The purpose of classifying functions, systems, and information is to differentiate them according to sensitivity and importance to safety and operations. The most resources should be allocated to the system and functions most important to safety and operations. It is beneficial if the classification system is standardized for the whole plant. The main criteria for the classification are the consequences if information is:

- Lost or destroyed.
- Unavailable.
- Used by or distributed to unauthorized users.
- Corrupted and distributed to users who are unaware of the corruption.

This implies that the classification of functions, systems, and information must not only take into account the importance, usefulness and "value" of the information as such, but also how this relates to the different categories of users. Plant data could, for example, have a different importance to operators and to maintenance personnel. This implies that the most effective way to allow different categories of users to use the same information could be through separate databases. The reason for this is that access control, back-up routines, and other data security measures may be differentiated according to the category of users and the information importance for each category of user. For example, safety related information that is used by the control room operators could also be of use to the maintenance staff in order to enable them to evaluate appropriate diagnostic activities. The information used by the operators will belong to a high safety class. In order to make the information available to the maintenance staff, the best solution might be to copy the higher class process database into a maintenance database belonging to a lower class. The purpose is to satisfy both the safety requirements and the information requirements in the most cost-effective way.

Guidelines and standards for safety classification, such as IEC 61226 [20] provide guidance on how functions and systems should be classified according to safety. In addition, guidance must also be provided for classification of the information stored, computed and distributed among different functions and systems. Rules have to be established on how information shall be protected regarding both, safety and the value the information represents. Such rules shall provide guidance for access (logical as well as physical), communication, storage facilities, back-up routines etc. in such a way that the security goals are reached to a reasonable cost.

7.4.4. Protection from loss of data and recovery routines

If information, despite protective measures, is lost or corrupted, recovery routines must exist in order to enable the reconstruction of the lost or corrupted data. Measures, such as protecting data communication and controlling both logical and physical access are preventive measures and a first line of defense. A second line of defense must exist if these measures fail.

One of the most important measures that must be taken in order to make it possible to recover from an incident, where data is lost or corrupted, is back-up routine. Depending on how important the information is and what damage a loss will cause, the following should be considered in advance before a back-up routine is established:

- Clear responsibilities must be established (who is responsible for making the back-up copy, who is responsible for the storage, who approves the use of an older version, etc.).
- It must be clear which functions, systems and databases should be included in the routine.
- It must be clear if the back-up should be automatically taken or if it should be manually initiated, or if both automated and manual back-up functions should exist in parallel.
- The back-up frequency must be clarified. Should a back-up copy be taken after changes and/or daily, weekly, monthly or yearly.
- It must be clear how many versions shall be kept.
- The storage media should be defined and tagged.
- It must be clear under what kind of circumstances an old version could be used.
- The routines to be used when an older version is put in operation must also be clarified in advance.

7.4.5. Data communication integrity

The integrity of computer networks and data transmission lines is one important factor contributing to the availability and correctness of information. Data security, as regards communication, should take into consideration the following issues:

- Availability — unplanned interrupts usually have a direct and negative impact on the application using the transmitted data. Data communication failures and interrupts in safety related communication networks may have consequences for the safe operation of the plant. Proper measures should be taken in order to avoid such events.
- Security — information can be obtained by unauthorized persons and used or manipulated against the nuclear power plant's interests.

There is a distinction between data security for communication networks under the control of the power plant, and public communication networks or networks owned or operated by a third party. The power plant does not have any jurisdiction over public networks or networks owned or operated by a third party. Because of this, it is necessary to set up rules that regulate what kind of information is allowed to be transmitted over such third party networks and how access to the plant internal networks should be controlled.

The following aspects should be considered in data communication:

- Need of data manipulation at the transmitting and/or receiving end.
- Encryption in order to protect data from unauthorized access.
- Use of firewall equipment or other types of interfaces in order to protect networks, systems or functions from unauthorized access and malicious intrusions.
- Policies and rules on which data can be used externally and how.
- Monitoring and control of the communication networks.

7.4.6. Access control

Both physical access to information through e.g. workstations, as well as logical access through public or open networks should be controlled and restricted.

The efforts put into access control must be balanced against the value of the information, which should be protected. This implies that information, systems, etc. of importance to the safe operation of the plant justify a higher degree of protection than administrative information widely used throughout the whole power plant. Sensitive business information may also need a high level of protection.

7.4.6.1. Physical access

The physical access to locations where workstations and other interactive interfaces are available should be restricted. The physical access to systems is recommended to be part of the general plant access control system.

Restrictions to physical access should include spaces where computer equipment such as hubs, routers, mainframes, etc. are housed. The restrictions should also apply for power distribution cabinets and supplies.

7.4.6.2. Logical access

Access to workstations and other interactive interfaces should be restricted. The access control system could require the use of, for example, keys and/or passwords. In some cases, when the use of such access control functions is impractical, workstations and other interactive interfaces could be open if other compensatory measures are taken. For example in the control room, the open access to the I&C systems and the HSI should be compensated with a more restrictive physical access control.

Unauthorized access could also take place through gateways from more open networks, for example plant office networks, inter-office networks or even public networks. In order to be able to take cost-effective measures, the needs of communications through open networks should be analyzed from a data security point-of-view. Based on the result of the analysis and the importance to plant safety and availability, proper protective measures should be taken. An example of such measures is to install barriers (for example firewall equipment or web-servers) between the different networks. The purpose of such barriers is to prevent unauthorized access from the more open network to the network with higher restrictions.

Passwords or a key could be used in many ways:

- Certain passwords may provide read-only access or access to specific applications.
- Personal passwords may be tailored to give access only to the applications needed.
- Keys in combination with personal passwords could permit computer access for a person without being at his own personal computer.
- Passwords and/or keys could also be used in order to allow access to external networks like the Internet.

The major benefit in using a password over simply a key is that it allows personal authorization. Due to its private characteristics, it is a cost-effective way to assure that only authorized persons are using the information available. In order to be effective, the use of passwords has to be well controlled and there should be a system in operation that forces the user to change his personal password regularly.

7.4.6.3. Information exchange restrictions

In principle information should only flow from a higher safety class to a lower. Logical isolation should prevent information from going from a network or function belonging to a lower class or category to a network or a function of a higher safety class or category. The logical isolation should in this respect act as a “check-valve” for the information flow. See IEC 61226 [20] for an explanation of safety categorization.

Isolation and integrity protection are especially important for the reactor protection system, which by definition belongs to safety category A. This means that a network or a function belonging to safety category A should be physically and logically isolated from other networks and functions belonging to a lower safety class or category (B, C or non-safety). The isolation should be made in such a way that information can flow only from the category A system or network to systems or networks belonging to a lower safety category. The isolation should also prevent any error or fault in the network or system belonging to a lower safety category from disturbing or corrupting data or functions in the category A system or network.

The needs of logical and physical isolation between systems belonging to safety category B, C and unclassified networks or systems have to be analyzed case by case.

8. TOOLS AND METHODS

8.1. INTRODUCTION

The use of tools can increase the integrity of the development process, and hence reliability, by reducing the risk of introducing faults. The use of tools can also have economic benefits as they can reduce the time and effort required in the design process.

Tools are either written or computerized methods. Their purpose is to facilitate the specification, design, development, and V&V of a system. When systems are designed, different types of tools are used. Some of the tools are more important for the integration of information than others. Examples are tools that support task analysis and modeling. Due to their importance to the integration of information, task analysis and modeling are described in more detail below. Computer aided design tools and software tools that are used to support software development, are described on an overview level only.

8.2. TOOLS SUPPORTING THE DESIGN PROCESS

To allow uniform processing as well as consistent data management throughout the various steps of the design, it is recommended to use different types of tools. The input information and source data for the tools used in the design process are, for example, the result of the different types of analyses performed in the early stages of the system life-cycle, e.g. task analysis. Other sources of input data for the design tools are the results of the modeling.

Tools are most efficient when they provide input for other tools used in later phases of the design process. An example is when the engineering tools provide data in a format usable for the code-generating tool. It is also beneficial if the output from the task analysis and modeling is in such a format that it can be used directly by the engineering and software tools.

The tools listed below are examples of software tools used to help develop, test, and analyze computer programs or their documentation.

- Compilers.
- Translators.
- Editors.
- Debuggers.

The software tools should support all or parts of the following steps in the development and design of software:

- Programming.
- Code generation.
- Documentation of the generated code.
- Testing and analysis of the generated code.
- Maintenance of the code and its documentation.
- Translation of formalized specifications, e.g. into application software (translation to another level of abstraction).

Guidance on the selection of the software tools can be found in IEC 880 [11] and in its future amendments.

8.3. COMPUTER AIDED DESIGN (CAD) TOOLS

Computer aided design (CAD) tools are used in the design of I&C systems. The CAD tools are used in order to support all aspects of the design of hardware (sensor installation, cabling, structure of boards in cabinets, etc.) and the interfaces between systems. Typical CAD tools are, for example, tools for drawing diagrams, tools for routing of cables, etc. It is beneficial if the CAD tools are able to interface to other tools used in the design process.

8.4. COMPUTER AIDED SYSTEM ENGINEERING (CASE) TOOLS

CASE (Computer Aided System Engineering) tools are very supportive of information integration. The main feature of the CASE tools is their ability to keep track of practically all types of data describing the information system design, such as data items, database structures, data relations, data flows, processes, different attributes, comments, functions, etc. The repository holding this information is unique for a project or a group of projects. This allows the CASE tool to organize cooperation between different project teams providing synergy effects. In order to benefit from the use of the CASE tool, it is necessary to implement it before I&C modernization or new systems are implemented.

8.5. ABNORMAL CONDITIONS AND EVENTS ANALYSIS (ACES)

IEEE 7-4.3.2-1993 [21] identifies the need for abnormal conditions and events analysis for software based systems. There are many techniques that can be used to support ACES analysis [22]. One example is failure modes and effects analysis (FMEA). It is used to identify as many as possible of the potential failures that can occur when a function is executed and the effects of this failure on the system. This methodology can be used in all phases of the development process. Tools exist to support FMEA analysis in several phases of the project.

8.6. TASK ANALYSES

Task analysis can be defined as a study of what operators and other users are required to do in order to achieve plant goals and the associated performance demands put on them. The task analysis should also identify all administrative and technical support needed to perform the task. The task analysis is supported by a number of specific techniques to help the analyst collect information, organize it and then use it to make various judgments and design decisions. The task analysis consist of several steps, where one step might be a hierarchical task analysis (HTA) describing overall goals which are decomposed down to single tasks. Another step, tabular task analysis (TTA), may then give all of the details for each of the single tasks.

The result of a task analysis should, as a minimum, provide the following information:

- A list of all tasks to be performed and by whom.
- Interconnections and relationships between tasks.
- Requirements on information needed to perform each task, including the definition of data to be used (existing, as well as new data).
- Need of technical support and interface capabilities for each of the tasks to be performed.
- A list of decisions to be made as a result of the performance of each task.
- Time needed to perform each task.
- Human actions and automated actions connected to each task.
- Environmental conditions.

Together with other inputs and constraints, the results of the analyses form the basis for the design and should be documented in a requirements specification. If the task analyses have been performed thoroughly, it will ensure that correct information is available in a timely manner when needed.

The performance of task analysis will also provide knowledge of the human involvement in the plant operation. This information can be used in order to evaluate if there is compatibility of the goals and objectives with the human and organizational capabilities.

In order to assure that the task analysis is effective, the methods for executing tasks should be analyzed. Careful consideration should be given to the knowledge, skills, and abilities required for accomplishing tasks to ensure that there are no gaps in the training, as it currently exists. Another essential element of the training for new systems is to focus on the differences between the old and new systems.

Several formal methods exist for the performance of a task analysis. A good overview of such methods is given in IEC 964 [9]. Cognitive user models may be needed to describe human performance limitations in time critical and complex tasks of information gathering/processing. Modeling has proved to be a useful tool in order to support task analyses, see Section 8.7 below.

When the tasks for each type of user have been identified, more detailed analyses have to be performed to provide knowledge for the basis for writing procedures and for the training of the staff. Another important activity that depends on a detailed analysis is the development of task- or job oriented formats. A typical approach in order to perform the detailed job analysis is to decompose each task into individual activities ("jobs") in order to be able to identify each individual step and action in, for example, a procedure.

8.7. MODELING

The purpose of modeling is to support the analysis, design, development, testing, and V&V of information presentation and human–system interaction. Another purpose is to identify constraints in specifications and proposed solutions. Modeling can also reveal hidden problems related to each task. The modeling can start early in the project to come up with a first conceptual design. The design should be driven by the user needs and based on plant goals and objectives instead of being technology driven. Therefore, considerable effort should be devoted to the early stage of the project with end-user involvement and feedback to capture and foresee the users needs.

Modeling can have a significant beneficial economic influence for the plant since it provides the ability to formulate and evaluate the user needs at an early stage of a project. This is more cost-effective and less complicated than to introduce changes at later stages of the project.

The models will also serve as a vehicle for carrying over the knowledge from one phase of the life-cycle to the next. The models become more detailed and comprehensive as they develop from the initial conceptual design to the final "as built" system. These models will constitute a part of the documentation for the whole development process.

There are a variety of modeling techniques available, ranging from various diagrams and flow-chart techniques, functional modeling, time sequence modeling, task analysis, visualization techniques (including virtual reality (VR) models) to the more analytical and cognitive models of human behavior. An overview of modeling human behavior is given in reference [23]. Considerable focus is now given to the functional modeling approach [24].

The user model is a practical approach for involving the users in the project. To provide the basis for the user oriented design, a detailed function and task analysis has to be performed, where the need of information for process monitoring and control for each user and task is identified, see Section 8.6. A framework for including the user model as a part of information exchange in the cognitive systems is given in Ref. [25].

After the user model, which describes the information needs, has been established, information modeling can be initiated. The detailed information modeling can start with a top-level layout of the control room describing the different function areas in the MCR. This includes the localization of workplaces for each user, local screens, panels and common information sources such as large screen displays.

The VR technique is a powerful tool for modeling the infrastructure, panels, and large screens in the workplace. It allows the user to comment and take a direct part in the design development. It is believed that it is the experienced operators, in continuous dialog with human factors experts and system and plant experts, that have potential to develop a well-designed control room. The methodology has been applied with good results in the Oscarshamn Unit 1 Modernization Project in Sweden [26]. In addition to the main control room, external facilities such as the technical support center, the emergency support center, and information to various off-site users should be included in the model.

The information presentation on the individual display screens should start with early prototyping to focus on establishing the rules for display format hierarchies, navigation principles, and the general layout. These basic rules should then be followed throughout the HSI design process.

When possible, the HSI should be prototyped on the same hardware and software to be used for implementation. This will make prototyping as realistic as possible and save time during the implementation phase. Prototyping can also be a starting point for the V&V activities, which should be an integral part throughout the whole design process.

As the prototype develops, more complex tasks and interactions can be modeled. This may require integration with dynamic simulators. In the final evaluation of the information model, a full-scope simulator may be needed to cover all aspects of human–system interaction.

9. EXAMPLES USING INTEGRATED INFORMATION

9.1. INTRODUCTION

The input of data, computation or treatment of the data and the output of the refined data to a consumer characterizes all information systems, including process I&C systems, control room information systems, administrative systems etc. In its simplest form, an information system has one data source, performs a simple computation of the data, and outputs it to one single consumer. More complex information- and I&C-systems require a higher degree of integration. The treatment and computation of data requires access to data and information from many sources. The output could be of interest to a broad spectrum of users. Modern technology in the areas of networking, data storage and access, data processing, and displays has brought about the ability to more thoroughly integrate information of diverse types and locations. This integration ability can be used to enhance the capabilities of systems in order to reduce human intervention between parts of a task or job, e.g. switching between different software applications or carrying out complex or long lasting tasks. This allows for greater productivity, offers higher performance, and reduces the risk of human errors.

All of the examples provided illustrate one or more aspects of information integration. The examples illustrate not only how information from many different sources can be combined and distributed in a nuclear power plant to enhance safety or efficiency of operation, but also highlight some of the measures which will facilitate the information integration making the use of computers more efficient, more robust, and less vulnerable.

9.2. INTEGRATED INFORMATION EXAMPLES

9.2.1. On-line emergency operating procedures

Commonly, emergency operating procedures are captured on paper and located in the control room for use by the plant operators. The operators watch the condition of the plant and evaluate a collection of plant parameters to determine if the plant is in a state requiring the application of emergency operating procedures. When it is determined that the plant is in a state requiring to be operated under the emergency operating procedures, the operator gets the procedures and applies them. This requires the operator to obtain information from various sources as required by the procedures and then following the procedures steps as indicated by the information. The information for following the procedures comes from diverse locations. It should be manually obtained, and in some cases processed, so that the correct actions in the procedures are taken. This process can be time consuming and error prone. Some potential errors are selection of the incorrect procedure, not recognizing when plant conditions change that cause a need to change to another procedure, obtaining the incorrect piece of information, or processing pieces of information incorrectly so that the resulting information is incorrect.

Integration and processing of information can be used to improve the above approach for handling emergency operating procedures. First the emergency operating procedures can be computerized so that they are readily available to the operator at his workstation. The plant data can be monitored by the system to determine when the plant goes into a state that requires the emergency operating procedures. It can also process the plant data to determine which procedure is appropriate and display that procedure. It can also continue to monitor the plant conditions and determine when it is necessary to change procedures. The system can then follow the procedure steps guiding the operator through them. It can also obtain all of the available information needed to make decisions in the procedures and display these values directly on the procedures where they are needed for monitoring and decision-making purposes. There may be some pieces of information, such as the location of a leak in the plant, which are not easy to obtain. In this situation, the system can prompt the operator to get the information. Here, the operator’s main job is decision making rather than information acquisition, information processing, and decision making. The operator can carry out his job more rapidly and more accurately with less likelihood for error.

Another example of the use of computerized procedures can be a plant safety monitoring and assessment system. In a conventional control room the operating staff are supposed to scan the indications, alarms, computer screens and make the evaluation of the plant safety status in their mind. This can be very tiring, monotonous, and provides the potential for human errors. In the case of an incident, the operators are supposed to identify the event, walk to the shelf and find the right emergency procedure (in paper form), find the right section in it and go through it step by step. This can be very time consuming and leads to the potential for more mistakes.

Using integrated information, a computerized monitoring system can be introduced. It can have an overview screen displaying the overall safety status of the plant, and the overall availability of the plant safety equipment. Behind the scenes critical safety functions can be evaluated based on their status trees. Should any deviation occur, the monitoring system can identify the exact symptom of the event and can select the needed emergency operating procedure. As it is also available in the integrated environment in an electronic form, the procedure text can be called to the operator’s screen starting at the needed first step. This whole process is very accurate, rules out human errors and gives the right instructions in a very short time. As the operator goes through the series of procedure steps, the system can log his actions for subsequent evaluation.

9.2.2. Work order activities

When maintenance is required on a piece of equipment, several things must be done in addition to the actual maintenance activity itself. In the past, all of these activities were performed manually. First the work order needs to be written, approved, and scheduled. The equipment out of service boundary is determined by looking at the drawings to determine which equipment needs to be taken out of service to safely perform the maintenance activities. Tags are then generated for both the equipment and the control room. The equipment within the tag-out boundary is shut off and tags are put on the equipment to indicate that they are out of service. Tags are also put on the controls in the control room to show that the equipment is tagged out of service. The maintenance work is performed, documented, and approved for return to operation. The equipment is returned to service and the tags are removed from the equipment and the controls.

Integration of information technology is used to reduce the effort and likelihood of error in this activity. The work order is written electronically with support of a work order system. Based on the needs identified in the work order the equipment out of service boundary can be generated automatically since plant information and relationships are captured in a knowledge base. The tags for the equipment and controls in the control room are automatically generated. The equipment is taken out of service and the tags are hung on the equipment and controls. The work order system can also interact with systems in the control room to mark the out of service equipment as unavailable in those systems. When appropriate these control room systems can automatically take into account that the equipment is out of service rather than the operator having to do this himself. After the maintenance is performed, the documentation can be put together and automatically stored. The equipment is put back into service and the tags are then removed. The work order system will then interact with control rooms systems to indicate that the equipment is back in service.

The computerized work order system will provide inputs for a database that can be used to analyze the fault history on both system and equipment levels. Information from the database can be used as input for the probabilistic safety analysis. This information can also be used to provide feedback on experience of component failures, which can be shared amongst the industry.

If the information in the work order database is integrated with the procurement system, purchasing of spare parts will be facilitated.

9.2.3. Plant transient analysis

Frequently engineering staff needs to perform plant transient analysis for several reasons. These include analysis for new fuel loading, diagnosis of plant transients, and evaluation of hypothetical situations. The first step is to develop a model of the plant or systems of interest. Plant drawings are used to obtain the information required for the physical part of the model. Voluminous calculations are required to take the information from the drawings and determine lengths, volumes, effective areas, etc. Equipment performance specifications and performance curves are used to get additional information for the model.

Heat transfer coefficients and other physical characteristics are found and made part of the model. The model is then developed and evaluated. The model is used to predict known benchmarks and previous plant transients. The engineer finds the initial conditions for the particular test, runs the simulation on the model, and obtains the results. He then compares the results obtained from the model with the results from the benchmark or actual plant transient. He probably also compares a prediction from the model of the current plant conditions with the actual plant conditions. Finally, after he is satisfied with the model, he performs the analysis desired. The results are then transferred or distributed depending on the type of analysis for future use.

The use of integrated information can greatly reduce the effort required to perform the above activities. The physical design data and performance information of the plant is captured electronically. Tools can be used to automatically generate the model of the plant for simulation based on input from the user. The initial conditions for the particular tests are also obtained automatically and put into the model. The engineers run the simulation and the results are automatically compared with the expected results, which have been stored from other applications. Similarly, he can obtain a prediction for current plant conditions and have the results automatically compared with actual plant data. When he is satisfied with the model, he performs the desired analysis. The results are automatically stored and documented for access by other user categories, which may need them for various purposes.

An important benefit of the plant transient analysis function is the ability to calculate whether an event is a full or a fractional transient. By using the data collected from the transient analysis, it is possible to calculate how much of the transient budget of a unit is used compared to the maximum allowed number of transients.

9.2.4. Remote diagnosis

Frequently equipment problems occur when the expert on the equipment is not at the plant. The expert was called to diagnose the problem, which required him to try to do it at his location or to come to the plant. For the purpose of this example, only the first case will be considered, but integrated information could eliminate the need for the second case. The expert is called and the situation is described. Any information he needs such as plant data, drawings, historical information, and maintenance records needs to be copied and transferred to him by fax, priority mail, or some other means. The expert studies the information. He may want some tests performed. In that case the information from the tests are collected, copied and again sent to the expert. Eventually he completes his diagnosis and actions are taken based on that diagnosis. If everything works as desired that may be the end of it; however, if things do not work as desired, the new information is collected and the cycle begins again. Potentially the expert may have to come to the plant to get enough information to perform the correct diagnosis.

Integrated information capabilities can reduce the effort and speed up the time to success substantially. Since information such as drawings, plant data, maintenance data, etc. are available electronically and can be integrated as needed, the expert can access the required information directly and promptly. He can request tests to be performed and can access the resulting information in real time to help his diagnosis or determine additional tests. Having complete and prompt access to all of the necessary information speeds up the process and increases the likelihood of success.

9.2.5. Equipment diagnosis and maintenance

Maintenance staff needs a wide variety of information when they go out to diagnose problems and perform maintenance activities. Frequently this includes: drawings, maintenance manuals, plant data — both current and historical, diagnostic information and other relevant resources. This information is needed by the maintenance person to perform the job. If some of this information is forgotten or not anticipated to be needed but is, then he either needs to return for it or request someone to bring it to him before he can complete the job.

Information integration supports the maintenance man in his diagnostic and maintenance activities in many ways. First, the maintenance man can carry a portable computer with him and hook it up to the plant information system. This will give him access to all of the information he needs without having to bring it with him or the delays in obtaining information not anticipated or forgotten. Second, diagnostic aids can be accessed to support the diagnostic activities. Third, he can directly interact with the work order system from the location of the equipment.

Information integration can also support joint investigations by combinations of the operations, engineering, and maintenance staffs. These joint investigations can be performed even if the participants are located in different geographical sites.

9.2.6. Fuel management and core surveillance

Before each new fuel cycle loading, a detailed core design and fuel optimization is performed by reactor physics specialists. They use design codes and tools licensed for use in safety analysis of the new core design. During outage the on-line core monitoring systems should be updated with parameters from off-line analysis for the new core design and positioning of fuel assemblies. It is extremely important that information management and data transfer between the different codes and systems are performed correctly, and that no errors are introduced in this process. Further, efficient coupling of off-line tools for core physics calculations and on-line modules in core monitoring can pave the way for cost savings.

Core monitoring and physics codes are becoming an integral part of the entire information system at the plants serving the reactor engineering group in core design, safety analyses and operation planning. During plant operation the control room operators rely on key information derived from on-line measurements and calculations for monitoring safety margins. Predictive simulations for planning operational maneuvers are used for real-time core control optimization. Core monitoring systems are gradually distributed to new user categories. It is not only the specialists in core physics and simulation codes that are users of the information that is produced from these advanced systems.

It is important to design flexible core monitoring systems that can easily be adapted to the different user needs and integrated with other plant information functions. With the increasing number of different computerized support functions, it is important that the core monitoring system is not seen as a stand-alone system, but rather can be seen as a natural part (e.g. unified human–system interface) of the entire information system. This is of particular importance for the control room operators. This is considered particularly important in the future where it is anticipated that core-monitoring systems will be expanded with new functions (e.g. information from technical specifications, procedures, noise analysis, etc.).

9.2.7. Management evaluation of plant status

Utility management, which is located off-site, may have various needs to know the current state of the plant and historical information of the plant to make decisions. The same can be said for the load dispatcher. In the past, the information available was usually obtained by a phone call and any additional analysis was either requested to be done by the plant or was limited to simple things that could be done with the limited information available. What-if evaluations of scenarios were difficult at best.

Under an integrated information environment, the plant information for both current state and historical periods is readily available off-site as appropriate. This allows real-time access by management to support their decision-making. It also allows various analyses and what-if scenarios to be performed without bothering the plant for additional information or analyses. This improves the quality and timeliness of the decision-making and improves the productivity at the plant since plant staff do not have to respond to the management requests for information.

9.2.8. Computerized control rooms

Development of advanced computerized control rooms can benefit from integrated information technology to a large extent. Some of the major goals are to optimize the entire HSI, to minimize the information load of the operator and to provide integrated procedures.

In contrast to a traditional control room, the operators do not need to move in order to perform control actions or to look for documents. Large mimic panels may provide the operating team with a global view of the unit status. To cope with a total loss of the primary I&C system (and hence the operability of all the primary functions in the control room), there can be back-up panels employing conventional (computer independent) equipment.

The main benefits that can be achieved from information integration in a computerized control room are:

- Fast and easy data access and interaction. Every mimic is put together in a way that each view contains all the data necessary to carry out the respective tasks. Additional details on the information in the mimic can be accessed easily.
- Assistance to determine reasons for malfunctions. A large amount of distributed information can be presented to the user via the displays. They can also provide information from the sensors and actuators, which is up-dated in real time, and other relevant data. This integrated information can help the operator understand the cause of the problem, e.g. locking, failure, loss of power supply.
- Alarm processing. State based processing of the alarms can be used to reduce the overload of the operator caused by the alarms during major transients and other plant states, e.g. loss of power, shut down of the plant. Files may be available for each alarm, providing the causes, the consequences, the risks, and recommendations for appropriate action by the operator in real time.
- Presentation of operating procedures and accident procedures. See Section 9.2.1.

- Examples of two integrated main control room designs are the N4 of Chooz in France [27] and the ABWR type control room of Kashiwazaki-Kariwa Units 6 and 7 of Tepco in Japan [28]. The designs of these two control rooms emphasize the need for a thorough analysis of operator needs in different plant states and the usefulness of large screens as a common overview information source in the control room to support team communication. Better support in disturbances with improved alarm systems and computerized procedure support are appreciated by the operators, as well as more task oriented operator support. They both report that operators show better performance with the new HSI compared to previous generations, and that training is very important in transition from old to new technology.

9.2.9. Plant safety information presentation at the licensing authority

The amount of the involvement of the licensing organization in the everyday operation of a nuclear power plant may vary from country to country. In some countries the authority may request periodic plant data, where periodic may mean virtually real-time, on-line information. In addition to this, a requirement for the availability of technical background information in a computerized form, such as drawings, operating manuals and plant procedures may exist for investigation purposes. The sources of this information may reside in several plant systems, e.g. the plant process computer, the core calculator, digital safety I&C systems, CAD systems, etc. Without information integration, these types of data can only be forwarded to the authority from the individual systems in separate pieces, and can be retrieved in separate applications on the other side.

Using information integration within the plant makes it possible to forward integrated data to users other than the plant operators. As the integrated environment is developed at the plant, the design may involve the transfer of plant information to office computers, for instance, to engineering workstations at the technical support organizations. One common way of doing this can be the application of WEB technology. In this case a WEB server will provide integrated information for several categories of on-site users. Using the same WEB technology, it is possible to access information from remote locations, such as the licensing body. The main advantage of this is that there is no need for specific presentation applications at the user site. The standard WEB browser, which is installed on virtually all office computers, provides the capability to display the integrated data from the plant WEB server. This way the licensing authority (and additional remote organizations, e.g. the utility headquarters) can access the requested information on-line, either via dedicated, point-to-point connections or via the Internet.

10. LESSONS LEARNED

10.1. INTRODUCTION

One of the most important lessons learned is the importance of the preparatory work done before the actual design starts. This preparatory work should include the establishment of the plant infrastructure plan, including a control room philosophy, and the analysis of the plant integration environment. The preparatory work should also include the identification of goals and constraints, and should then continue with more detailed analyses. After a project is initiated, it follows the project life-cycle. The lessons learned listed in this section are organized according to this life-cycle.

The findings evolved from presentations and discussions of the authors' contributions to this report, the examples presented therein, and from the papers and discussions of the IAEA specialists meeting on the subject in Stockholm, May 2000 [29].

10.2. LESSONS LEARNED IN THE VARIOUS SYSTEM LIFE-CYCLE PHASES

10.2.1. Preparatory work before the life-cycle of an individual project

- When integrating new operator support systems, inconsistencies between the engineering and information management tools for different applications often lead to poor performance caused by inconsistent or incompatible interfaces.
- Not having a set of guidelines for HSI design may cause inconsistencies with the potential consequence of increasing human errors.
- Problems resulting from the evolution of non-integrated I&C systems have a detrimental effect on the performance, connectivity, and maintainability of the systems and their information.
- Stepwise implementation of new I&C functions, if not handled properly, can lead to a lack of system integration in the control room, and inconsistencies and inefficiencies in general.

10.2.2. Project initiation, goals and constraints

- Incomplete or not updated documentation requires a recapture of the design basis.
- After the plant has been built, changes in safety requirements have made it necessary to reconsider the safety system design process.
- Not engaging the operators early in the project has led to operators' resistance to changes.
- Not having adequate resources allocated for the project has led to insufficient performance and/or poor quality of the system.
- Technology driven solutions do not satisfy user needs in many cases.

10.2.3 Project preparation and feasibility study

- Modernization of I&C systems may lead to increased number of redundant trains, requiring changes in training, procedure writing, etc.
- Poorly designed HSIs in control rooms do not facilitate team communication.

10.2.4. Overall system architecture and basic requirements specification

- Mixtures of old and new technology in the control room, if not designed properly, may lead to human errors, and special attention should be paid to overlapping information.
- Increased amount of data that is not presented properly could lead to overloading the user.

- The use of VDUs only may cause a focus on details (tunnel effect) and the loss of a comprehensive understanding of the plant situation and status.
- Introduction of improved alarm systems often leads to integration problems with respect to the existing information environment.
- If appropriate measures are not taken to protect the different systems and functions, data corruption may occur.
- When information is not organized in a way that maintenance and operations activities are clearly separated, the operator may be hindered by maintenance or non-operators’ activities.

10.2.5. Detailed requirements specification for individual systems

- In many cases standard HSI solutions offered by the vendor, when the requirements specifications have not been performed in an iterative manner between the vendors and the plant users, have not fulfilled the functional requirements.
- The vendors usually do not have operating experience, while the users usually do not have design experience, so this should be recognized and considered in the iterative specification and design process.
- Since operators spend a substantial amount of time in front of the display screens, it is important to design the working environment, e.g. ergonomics, illumination, etc. to avoid fatigue and thereby optimize operator performance and productivity.
- If analyses were not performed thoroughly enough, it has been observed that users have to move back and forth unnecessarily between different systems when performing a job or a task.
- Alarm systems often cause problems when the operating state deviates from normal conditions, such as, information overload of the operators from too many alarm messages generated during transients.

10.2.6. System realization

- If documentation is not consistent with the as built status of the system, it can be detrimental to safety and/or economics and will make the implementation of new systems or functions difficult. Computerized documentation facilitates keeping the documentation consistent and easily accessible.
- Where documents are produced via different engineering processes or tools, a lack of configuration management tools has led to inconsistency.

10.2.7. Implementation, operation and maintenance

- V&V of the HSI often comes in at the very end of the project when it is too late or too expensive to make changes.
- Changing from analog to digital requires new skills for the maintenance staff.
- Systems initially implemented with poor quality and inadequate functionality have caused users to reject the system.
- Inadequate simulator and other training have required substantially more time and effort to reach adequate knowledge and skills of the staff.

11. RECOMMENDATIONS

The recommendations from this report, grouped by sections, are given below.

Plant infrastructure plan and plant integration environment

- A living, plant specific, long term plant infrastructure plan, including control room philosophy, should be developed based on the needs and constraints of the plant as a whole.
- A living, plant specific communications model to identify and describe the information and protocols to pass that information should be developed.
- A living, plant specific data model to define the structure of the plant data should be developed.
- A living, plant specific plant integration environment to facilitate the access to distributed pieces of information, access to distributed functions, and the tools to integrate both the information and functionality should be developed.

Analysis of needs

- All necessary analyses should be performed in a timely manner to avoid expensive corrections in the later phases of the project, and these analyses should be documented so that documentation is usable for other applications as well.
- Resources allocated to the project should be sufficient to successfully implement the system consistent with the recommendations of the analyses and to satisfy the overall goals with the final system.
- Methods should be used to evaluate the impact of modifications on the control room to ensure that the modification will not degrade the overall control room performance.

Mapping the systematic approach to a system life-cycle

- Design and development of systems should follow a systematic approach, such as given in established life-cycle guidelines.
- The goals of a project should take into account the needs and constraints on information integration by mapping the project to the long term plant infrastructure plan.

Important issues for information integration

- A human system interface plan should be established to identify all users' categories, users' needs and interfaces to other systems; and to identify and manage all aspects of an I&C change that has an impact on humans from the new or modernized system. An HSI group should be established to manage the human–system interface plan.
- The human system interface should be designed such that the operators are always aware of the actual state of the plant and are never exposed to information overload, even in the case of the worst plant disturbances. Arrangements of

workplaces, display screens, and instrument panels should support team communication and sharing of information.

- Task oriented information presentation should be supported and encouraged in the HSI design.
- Efficient navigation functions in large display systems consisting of several hundred pictures should have properly designed display hierarchies, and other required capabilities to support timely performance of users' tasks.
- A data security policy should be established. This policy should be taken into consideration when the plant infrastructure plan and plant integration environment are produced.
- Only authorized people following established procedures should be allowed to enter data into systems to help ensure the quality of data.
- Information should only flow from a higher safety class to a lower safety class to prevent information corruption.

Tools and methods

- Appropriate tools should be used to increase the integrity of the development process, to increase quality and to reduce time and cost.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, Vienna (1998).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues for Advanced Protection, Control and Human–Machine Interface Systems in Operating Nuclear Power Plants, Safety Reports Series No. 6, IAEA, Vienna (1998).

[3] ELECTRIC POWER RESEARCH INSTITUTE, Plant Communications and Computing Architecture Plan Methodology, EPRI-TR-102306, Vols 1&2 (1993).

[4] ELECTRIC POWER RESEARCH INSTITUTE, Plant Communications and Computing Architecture Plan Methodology — Revision 1, EPRI-TR-104129, Vols 1&2 (1994).

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, ISO/IEC Standard 7498-1, (1994).

[6] ELECTRIC POWER RESEARCH INSTITUTE, Utility Communications Architecture, EPRI EL-7547, Vols 1–6 (1991).

[7] ELECTRIC POWER RESEARCH INSTITUTE, Database Access Integration Services (DAIS). EPRI TR-101706, Vols 1&2 (1992).

[8] ELECTRIC POWER RESEARCH INSTITUTE, Plant-Wide Integrated Environment Distributed on Workstations (Plant-Window) System Functional Requirements, EPRI-TR-104756 (1996).

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Design for Control Rooms of Nuclear Power Plants, IEC-964 (1989).

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, IEC-61508 (1999).

[11] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, Rep. IEC-880, Geneva (1986).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear power Plants, Technical Reports Series No. 282, IAEA, Vienna (1988).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Specification of Requirements for Upgrades Using Digital Instrument and Control Systems, IAEA-TECDOC-1066, Vienna (1999).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, Technical Reports Series No. 384, Vienna (1999).

[15] NUCLEAR REGULATORY COMMISSION, Advanced Human–System Interface Design Review Guideline, NUREG/CR-5908, US Govt. Printing Office, Washington, DC (1994).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Automation and Humans in Nuclear Power Plants, IAEA-TECDOC-668, Vienna (1992).

[17] NUCLEAR REGULATORY COMMISSION, Guidelines for Control Room Reviews, NUREG-0700, US Govt. Printing Office, Washington, DC (1981).

[18] FARBROT, J., BYE, A., BERG, Ø., "How to build a better alarm system for your NPP", Paper presented at the IAEA Specialists' Meeting on Integrated Information Presentation in Control Rooms and Technical Offices at NPPs, Stockholm, 2000.

[19] CARRERA, J.P., EASTER, J.R., ROTH, E.M., “Simulation Testing of the Westinghouse AWARE alarm management system”, (Proceedings IAEA Specialists mtg on Experience and Improvements in Advanced Alarm Annunciation Systems in NPPs, Chalk River, Canada, 1996.

[20] INTERNATIONAL ELECTRO-TECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important for Safety — Classification, IEC-61226 (1993).

[21] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-1993, IEEE, Piscataway, NJ (1993).

[22] ELECTRIC POWER RESEARCH INSTITUTE, Abnormal Conditions and Events Analysis for Instrumentation and Control Systems, EPRI TR-104595, Vols 1&2 (1996).

[23] CACCIABUE, C.P., Modeling and Simulation of Human Behavior in System Control, Springer, London (1998)

[24] BYE, E., HOLLNAGEL, BRENDEFORD, T.S., Human-machine function allocation: a functional modeling approach, Reliability Engineering and System Safety **64** (1999). 291–300.

[25] BYE, A., HOLLNAGEL, E., HOFFMANN, M., MIBERG, A.B., “Analyzing automation degree and information exchange in joint cognitive systems: FAME, an analytical approach”, Paper presented at 1999 IEEE international conference on Systems, Man and Cybernetics, Tokyo, 1999

[26] GUNNARSSON, T., FARBROT, J.E., “The integrated control room development process on Oskarshamn O1 NPP modernization project”, Paper presented at IAEA Specialists Meeting on Integrated Information Presentation in Control Rooms and Technical Offices at NPPs, 2000, Stockholm.

[27] DOUTRE, J.L., PIRUS, D., “N4 NPP’s operation: Preliminary tendencies”, EHPG meeting, Lillehammer, Norway, 1998.

[28] KAWANO RYUTARO, FUJIIE MINAKO, OHTSUKA TSUTOMU,“Evaluation of human-machine interface of the ABWR type control room panel based on operators’ behaviors and subjective data”, Cognitive Systems Engineering for Process Control (CSEPC’96), 1996, Kyoto, Japan (1996).

[29] IAEA Specialists Meeting on Integrated Information Presentation in Control Rooms and Technical Offices at Nuclear Power Plants was held in Stockholm, Sweden, 2000.

CONTRIBUTORS TO DRAFTING AND REVIEW

Anderson, O.	Forsmark Kraftgrupp, Sweden
Berg, O.	OECD Halden Project, Norway
Eiler, J.	Nuclear Power Plant Paks, Hungary
Ki-Sig Kang	International Atomic Energy Agency
Kossilov, A.	International Atomic Energy Agency
Kostika, F.	CEZ-NPP Dukovany, Czech Republic
Naser, J.	EPRI, United States of America
Poizat, F.	Electricite de France, France